Section 30—Scope of Work

In this RFP, the word "shall" means mandatory.

If a vendor does not comply with the directives contained in the various provisions of this RFP as noted by the word "shall", then the vendor's entire Response shall be deemed "non-responsive" and not be further considered or evaluated by the Commonwealth.

In this RFP, the word "should" means non-mandatory.

If a vendor omits or does not fully respond to a provision in the RFP as noted by the word "should", the specific omission or incomplete response will NOT be deemed to render the entire Response "non-responsive" so as to eliminate the vendor from further consideration and evaluation by the Commonwealth. By not responding to a provision noted by the word "should", the vendor will not be awarded any points for that provision. If the vendor does respond to a provision noted by the word "should", that vendor will be evaluated in accordance with the evaluation criteria set forth in the RFP.

Vendors please note that the scoring methodology that will be utilized by the Commonwealth in evaluating all proposals is based upon the Commonwealth's understanding of the current market.

In provisions noted by the word "should", vendors may propose equipment, software, or services available in the market which further the goals of the Commonwealth previously expressed in this paragraph. Thus, Vendors will be rewarded with points for proposals that achieve these goals for the Commonwealth.

Scope of Work Section Description

The Cabinet for Health and Family Services (CHFS), Department of Medicaid Services (DMS) desires to select a Vendor(s) to perform a specific set of activities to support:

1. Design, development, implementation and maintenance of the Kentucky Medicaid Enterprise Management System (MEMS) and Fiscal Agent (FA) services as defined in Section 30.060 of this RFP. In addition to the system and FA services, the MEMS System Hosting and Disaster Recovery services, a Decision Support System (DSS), and Utilization Management Services are included as "Options to Buy". This provides the Commonwealth the option to award those services to the prime Vendor or to pursue alternative solutions (Replacement)

2. Planning, migration and operations necessary to assume the operation of the current MMIS and FA services as defined in Section 30.070. (Takeover)
3. Providing of all services necessary for Options 1 & 2. (Takeover and Replacement)

This section identifies the scope of work requirements for Options 1 and 2. It is important to note that this Solicitation reflects current knowledge. Vendors should be prepared to adapt and respond to changes that arise from Federal updates, future regulations, and associated policy decisions on behalf of the Commonwealth. Such changes should not be considered a change in the overall scope of work.

Option 1 – Replacement System

A. The replacement system should meet all of the requirements for performing MMIS activities and ongoing maintenance as indicated in this RFP, in addition to the functional and technical requirements detailed in Appendix A - MEMS Functional Requirements and Appendix B - MEMS Technical Requirements. Detailed requirements gathering as part of this scope of work should further refine/define the requirements for this solution. These requirements should be the basis for the selected Vendor to create usage scenarios and detailed business process workflows. However, at the conclusion of the detailed requirements phase, the Commonwealth expects the selected Vendor to work with the Commonwealth team to prioritize requirements and if necessary, identify possible phases for implementation of the overall requirements. The selected Vendor's Project Work Plan should be updated to identify all possible phases of implementation.

B. As part of the Replacement option, the Commonwealth requests Vendors to respond to "Options to Buy" which may or may not be exercised within the contract. The Commonwealth requests that the Vendor propose a solution for each "Option to Buy" and include the costs for each item separately in the Cost Schedules detailed in Section 70. The "Options to Buy" are identified within the subsections of the RFP, as indicated below:

    1. Section 30.060.260.010 – System Hosting and Disaster Recovery Services
    2. Section 30.060.260.020 – Decision Support System (DSS)
    3. Section 30.060.260.030 – Utilization Management (UM) system

C. The Commonwealth seeks a best of breed approach for procuring the overall solution for the MEMS and understands this may include products offered in a variety of ways as part of an integrated solution. In order to provide a flexible and innovative framework, the MEMS is a key component to a fully-integrated Kentucky Medicaid program.

    CHFS has developed a technological roadmap for the Kentucky Quality Health Information (QHI) framework. The QHI facilitates the implementation of

technology standards and approaches for the development of an interoperable, scalable and easily adaptable cross-sector technology framework.

Kentucky views the QHI as a house built on a solid foundation of a sharable technical services and a common enterprise service bus with various applications as pillars. Details regarding the QHI can be found in section 30.060.240.030.

D. In its proposal, the Vendor should clearly demonstrate understanding of the division of functions in the MEMS Operating Model, Appendix E to this RFP.

The Operating Model represents the combined vision for the operation of the interdependent functions of the MEMS Solution. Included in the operating model are: administrative functions to support oversight and operations; financial management functions to ensure financial viability of the MEMS and to support the administration of financial programs and the processing of financial transactions.

E. Stakeholders foresee an environment that utilizes advanced technology and multiple channels to reach an array of users. The MEMS channels should include online capabilities offering MEMS functions via an online portal that is accessible through a standard or mobile web browser. The Self Service Portal supports communications between customers and the MEMS, including web chat and, email. A toll free hotline should provide customers with the opportunity to access information via an Interactive Voice Response (IVR) or direct conversation with a Medicaid worker. This interfaces with the Contact Center which is being developed as part of the HBE. Paper publications that provide education and access to the MEMS may be mailed on request or printed directly from the Self Service Portal. The MEMS is also considering using outbound text messaging for notifications or alerts and voicemail functions for outbound call campaigns. Finally the MEMS should support channels for direct system-to-system communication, including support for service-enabled devices through web services interfaces that enable data exchange between third parties and regulatory bodies like HHS, IRS, and other State Agencies. Where required, communication channels should be accessible to people with disabilities in accordance with the Americans with Disabilities Act and section 508 of the Rehabilitation Act and should provide meaningful access for persons with limited English proficiency.

F. The MEMS solution should adhere to architecture guidance and the seven conditions and standards for enhanced Federal funding as provided by CMS. In alignment with this guidance, the technical solution architecture should employ a modular design, based on Service Oriented Architecture design principles and the Medicaid Information Technology Architecture (MITA) framework. The following sections address this solution approach and identify the technical requirements by each layer in the application architecture design.

Option 2 – Takeover of KYMMIS System

A. Takeover includes the activities required to successfully transfer, configure, install, test, and implement KYMMIS for the Commonwealth and assume responsibility for its ongoing operations and maintenance.
B. The KYMMIS Vendor should conduct a detailed survey and analysis of the current KYMMIS, including the operation and maintenance of the KYMMIS, current procedures, work in progress, outstanding work, and user requirements in finalizing the Work Breakdown Structure (WBS) required as part of the Vendor's technical proposal.
C. The KYMMIS takeover activities should include, but not be limited to, processing tests and an operational readiness review sufficient to demonstrate that the KYMMIS Vendor is ready to begin operations for each and every function.
D. DMS must approve the KYMMIS Vendor's operational readiness test before the initiation of the KYMMIS production operations. In the event DMS does not approve the start of the KYMMIS Vendor's production operations, the Vendor should be responsible for making arrangements to continue the FA and IT operations. The KYMMIS Vendor will operate and maintain a federally-certified MMIS. The KYMMIS Vendor shall be liable for damages incurred by the Commonwealth.

Option 3 – Combination Replacement MEMS and Takeover of KYMMIS System

Vendors may choose to propose both the Takeover of the current KYMMIS and the design, development and implementation of the Replacement MEMS. The proposals for each option are scored separately. Price proposals for Option 3 must include separate pricing for each option as well as a total cost if both are awarded to the Vendor. The Commonwealth may choose to award Option 1, Option 2, or both depending on the final scoring of all Vendor proposals.

Section 30.005—Commonwealth Information Technology Forms

The Vendor and any subcontractors shall be required to adhere to and sign all applicable Commonwealth policies and standards related to technology use and security.

Section 30.010—Compliance with Commonwealth IT Enterprise Architecture and Standards

The Commonwealth IT Enterprise Architecture and Standards reflect a set of principles for information, technology, applications, and organization. These standards provide guidelines, policies, directional statements and sets of standards for information technology. It defines, for the Commonwealth, functional and information needs so that technology choices can be made based on business objectives and service delivery. The Vendor shall stay knowledgeable and shall abide by these standards for all related work resulting from this RFP.

Web link: **http://technology.ky.gov/governance/Pages/architecture.aspx**

Section 30.020—Compliance with Commonwealth Security Standards

The software deployment and all Vendor services shall abide by security standards as outlined in the Commonwealth's Enterprise Information Technology Policies.
Enterprise Policies
http://technology.ky.gov/ciso/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx

Section 30.030—Privacy, Confidentiality and Ownership of Information

DMS is the designated owner of all data and shall approve all access to that data. The Vendor shall not have ownership of Commonwealth data at any time. The Vendor shall be in compliance with privacy policies established by governmental agencies or by State or Federal law. Privacy policy statements may be developed and amended from time to time by the Commonwealth and should be appropriately displayed on the Commonwealth portal (Ky.gov). The Vendor shall provide sufficient security to protect the Commonwealth and DMS data in network transit, storage, and cache.

Section 30.040—Software Development

Source code for software developed or modified by the Vendor specifically for the Commonwealth shall become property of the Commonwealth.

Section 30.050—License Agreements

Software provided by the Vendor to the Commonwealth shall contain a provision for perpetual licensing with all upgrade options. The Commonwealth may decide to maintain the software in escrow; therefore the agreements shall also contain a provision for maintaining a version of the software in escrow in the event the Vendor is unable to continue the business for financial or other business reasons.

Section 30.055—Identity Theft Prevention and Reporting Requirements

The selected vendor is responsible any mitigation, cleanup and reporting costs from Identity Theft, system breach or breach as defined under the HIPAA Privacy Rule. For even a single knowing violation of these Identity Theft Prevention and Reporting Requirements, the vendor agrees that the Commonwealth may terminate for default the contract(s) and may withhold payment(s) owed to the Vendor in an amount sufficient to pay the cost of notifying Commonwealth customers of unauthorized access or security breaches. The Vendor must attest/certify to CHFS that it has established and will share a breech notification policy and program.

Section 30.058—Vendor Selection

The CHFS seeks to award a Contract to a knowledgeable and responsive Vendor having experience in the development and implementation of statewide web-based multi-layered integrated MEMS. The selected Vendor should provide innovative, cost-efficient and appropriate business management and technology solutions for designing, developing and implementing the envisioned software.

The Commonwealth is seeking a Vendor that is responsible for providing a complete software solution and all requested services required for a successful implementation, plus post-implementation support, and possible long term operational support for the Medicaid Enterprise Management System. The Vendor may team with multiple firms in its proposal, but there can be only one Vendor that executes the Contract expected to result from this RFP. This does not preclude the State from executing a separate contract with a Software Provider for software licenses and software maintenance. However, the Vendor is responsible contractually for all services, including those services performed by a sub-contracted software provider.

The Vendor should coordinate, integrate, and be accountable for all products and services proposed. This excludes an arrangement between Vendors of joint venturing or joint response to this RFP as such arrangements are not allowed. Generally, the Vendor may only appear in one proposal submitted in response to this RFP. Subcontractors may be included in more than one proposal. Multiple submissions from a firm that is a Vendor in a proposal or submission of alternative proposals will be grounds for disqualification of such proposals.

This restriction does not apply to products or software. This means that a software provider may also offer its services as a Vendor, serving as its own integrator, and another Vendor can offer the same software in another proposal. In this latter case, the affected Software Provider cannot also serve as a Service Provider in any proposal other than the one in which it is the Vendor.

At the sole discretion of the Commonwealth, submitting multiple proposals in different forms may result in the disqualification of all Vendors knowingly involved.

Section 30.058.010—Vendor Experience Requirements (Sections 60.010.010.030; 60.020.010.030)

The Vendor or subcontractor selected for this initiative should have:

1. A clear, complete, and comprehensive vision for the direction of the business.
2. Evidence of fiscal stability, including being able to demonstrate that this project will not have a material impact on the Vendor organization’s financial status.
3. Recent experience (past five years) designing, developing and implementing a large enterprise system.
4. Recent experience providing fiscal agent services.

The Vendor demonstrates that their company has the relevant experience providing the services defined in this RFP, and that the staff proposed for positions on this Project

have the appropriate knowledge and experience obtained on Projects of similar nature, size, and scope. CHFS may require substitution/replacement of any key personnel assigned to the Project if it determines that person does not possess the skills necessary to satisfactorily complete the activities assigned.

The successful Vendor should have a minimum of five prior years experience in the delivery of services on projects involving the design, development, and implementation of large systems. Experience preferably should be within the last five years, although earlier experience may be submitted if it demonstrates continuity of services over a broad span of years. The Vendor identifies any experience with Federal requirements for Medicaid programs and/or MMIS, or other Federal programs such as HIPAA, Food and Drug Administration (FDA), HBE, or related service areas.

The Vendor should provide information regarding any similar or major project they have participated in over the past five years that was they did not completed or was cancelled. Information should include the reasons for the incomplete or cancellation. Lessons learned from this experience should also be shared.

Section 30.058.020 – Value Added Services (Section 60.010.010.140)

Value-added services provide additional functionalities and capabilities that enhance a Vendor's solution. This is an opportunity for Vendors to distinguish themselves from competing Vendors. The Vendor should recommend, in summary format, innovative Practices, Business Strategies and value-added services that should be offered by the Vendor to enable the Commonwealth to be successful in this effort.

Section 30.059 – Independent Verification and Validation

The selected Vendor should cooperate with any Third Party Vendor(s) that the Commonwealth engages for the purposes of Independent Verification and Validation (IV&V) of the Program or system at any point in the program life cycle. The selected Vendor should, upon request and as required, provide documentation to CHFS and the IV&V Vendor to facilitate the independent verification process. The MEMS Vendor should support the IV&V Vendor in its objective verification and validation activities. The IV&V Vendor should have access to all deliverables and visibility into the MEMS Vendor's processes to produce those deliverables, including on-site visits.

The most significant contribution expected of the IV&V consultant is performing project oversight and acting in the role of a contract monitor to oversee the contractual obligations, performance, and compliance of the Vendor awarded the RFP for the new MEMS. CHFS views the function of the IV&V consultant as literally independent, and not a part of the DDI process. The IV&V consultant should be able to sample, review, and critique all parts of the Vendor's DDI activities and the CHFS's oversight of those activities.

CHFS and the IV&V consultant will review all deliverables of the selected Vendor. The deliverables should be defined in the RFP along with a description of the formal process to be used in the submission and review of the deliverables. The implementation

Vendor should produce and submit to CHFS/IV&V deliverables based on the dates that are agreed upon in the project schedule.

The IV&V will independently produce status reports on the progress of the project and submit them simultaneously to CHFS and CMS. This action should ensure a check and balance approach to assessment and allow the IV&V consultant to maintain the independence it needs to do the job for which they were contracted. It should also ensure that CMS is getting necessary information in a timely and unedited manner. CHFS will also initiate a standing monthly status update call with CMS the week following the status report to discuss the findings, recommendations, and corrective action, if required.

Section 30.060—Replacement System Scope of Work

The Scope of Work (SOW) for the implementation of the new MEMS calls for the Vendor to:

1. Propose and develop a system using a modular design and interoperable enterprise architecture employing a collaborative teaming approach. The Vendor should provide services required to maintain, enhance and operate the new MEMS over the Project Life Cycle (PLC). The replacement system will meet the applicable Medicaid Enterprise Certification Toolkit (MECT) requirements, align with MITA, and comply with the CMS Seven Conditions and Standards. Kentucky's functional and technical requirements are identified in Appendix A – MEMS Functional Requirements and Appendix B-MEMS Technical Requirements. The Vendor should meet these objectives by executing the following activities:
    a. Activity 1 – Project Management.
    b. Activity 2 – Detailed Requirements Analysis.
    c. Activity 3 – Design.
    d. Activity 4 – Development.
    e. Activity 5 – Data Conversion.
    f. Activity 6 – Business Process Transition.
    g. Activity 7 – Acceptance Testing.
    h. Activity 8 – Training.
    i. Activity 9 – Implementation.
    j. Activity 10 – Operations – Fiscal Agent.
    k. Activity 11 – Certification.
    l. Activity 12 – Software Maintenance and Modification.
    m. Activity 13 – Turnover.
2. Recommend the integration of best-of-breed existing and proven products rather than the traditional approach to new systems development that includes a state-of-the-art modular framework and supporting services, e.g., rules engine and workflow management, from best-of-breed Vendors. (Activities 1, 2, 3, 4, 5, 7, 9).
3. Prepare the MEMS for Federal certification and to conduct planning activities to assure the new MEMS is developed and enhanced to meet MITA in Activity 11.

4. Provide FA Services to operate the MEMS for an 8-year period (5 base years and 3 optional years) to meet the operations requirements identified in Activity 10.
5. Software maintenance and modification should be provided as part of the base contract for an 8 year period (5 base years and 3 optional years) to meet the operations requirements identified in Activity 12.

The scope of the MEMS requirements includes the major functionality/modules and system components that are defined in Appendix A – MEMS Functional Requirements and Appendix B – MEMS Technical Requirements.

The Scope of Work defines the activities to be performed by the Vendor to develop and implement a new MEMS that meets DMS requirements including the activities for FA Operations (Activity 10) and Software Maintenance and Modifications (Activity 12) of the MEMS after implementation. The Scope of Work assumes the following:

1. The Vendor should provide/develop a system to meet the functional requirements defined in Appendix A – MEMS Functional Requirements and as specified in Activities 1 through 12.
2. The Vendor should assist DMS in the development and implementation of new business processes and workflows as defined in Activities 3 & 6.
3. The Vendor should provide DMS training as defined in Activity 8.
4. The Vendor should provide FA services as defined in Appendix A –MEMS Functional Requirements, and as specified in Activity 10.
5. The Vendor should assist the Commonwealth in the Certification Readiness Effort with planning and expertise defined in Activity 11.
6. The Vendor should provide Software Maintenance and Modification following MEMS Implementation as defined in Activity 12.
7. The Vendor should provide Turnover services as defined in Activity 13.

Section 30.060.010—CHFS General Responsibilities

CHFS general responsibilities are:

1. Provide overall project direction and management.
2. Provide input and clarifications to the Vendor for developing the Deliverables.
3. Provide access to CHFS policies and procedures related to Vendor Deliverables. When applicable, provide access to appropriate staff to clarify requirements consistent with the MEMS Requirements Definition Report.
4. Attend deliverable walk-throughs to enhance understanding and facilitate the approval process.
5. Review and provide comments on draft Deliverables.
6. Review and approve Deliverables.
7. Ensure that technical assistance and support are provided in capacity planning, network planning, database and dictionary requirements, and software requirements of any existing (package) or developed systems.

8. Establish project organization by meeting with Vendor project management to finalize and document areas of responsibility, personnel reporting relationships, and administrative procedures.
9. Establish evaluation mechanisms by setting up procedures for day-to-day control of the Project as defined by the combined CHFS and Vendor project management team.
10. Coordinate other CHFS resources as needed to support the development and implementation process.
11. Provide information and answer questions at Vendor request.
12. Assist the Vendor in closing out action items.
13. Provide a project team consisting of a Program Director, technical staff, and business analysts representing the business areas throughout DMS. In addition, part-time participation from other CHFS staff should be available as defined in Appendix I – Commonwealth Responsibilities and MEMS Project Team Composition. The Vendor should consider these staffing levels when developing the resource management portion of the Project Plan.
14. The CHFS Program Director ensures that the Project is in compliance with the Contract and satisfies the requirements stated in the RFP. The CHFS Program Director will consult with the Project Sponsor on a continuing basis on every activity of the Project. This coordination should ensure that the new MEMS is properly designed, tested and implemented, supports the defined functional and technical requirements contained in the RFP, and is properly documented.
15. The standard turnaround for CHFS review of deliverables should be 15 work days and may be extended if CHFS determines in its sole discretion that it is necessary. CHFS encourages early submission of draft documents to expedite CHFS review. If the deliverable is not accepted, the Vendor will have 10 days to make necessary corrections and resubmit. CHFS will have 15 days to re-review.
16. Monitor Vendor performance.

Section 30.060.020—MEMS Vendor General Responsibilities

MEMS Vendor general responsibilities are:

1. Provide/develop a system to meet the functional requirements defined in Appendix A – MEMS Functional Requirements and Appendix B – MEMS Technical Requirements.
2. Provide training services for Vendor and DMS users and Providers as defined in Activity 8.
3. Provide FA and quality management support services to DMS and the new MEMS that ensure, and maintain the integrity of customer and stakeholder relationships and program performance as defined in Activity 10.
4. Provide Operations and Maintenance Support for the new MEMS system components as defined in Activity 12.
5. Submit written status reports to the CHFS Program Manager as defined in Appendix G – Deliverables.
6. Obtain CHFS written approval of the Project Plan.
7. Obtain CHFS approval on deliverable formats prior to completing deliverables.

8. Ensure that deliverables submitted to CHFS meet the deliverable requirements.
9. Obtain written approval from CHFS on deliverables before it will be considered completed.
10. Perform internal quality control on deliverables before submission for CHFS review and maintain records of those activities.
11. Provide information and support to the Independent Verification and Validation (IV&V) Vendor involved in the quality assessment of the MEMS development and implementation activities.
12. Attend meetings and present Project status as directed by CHFS.
13. Provide facilities and equipment as defined in Appendix G- Deliverables.

Section 30.060.030—Project Staffing (Section 60.010.010.130)

A key factor in the success of the project is the degree of collaboration between Project staff, CHFS participants, and Vendor staff. The Vendor's Project team is responsible for performing and supporting the project with quality-related activities described throughout this Section of the SOW. CHFS expects the Vendor to staff the project team with individuals who have expertise to perform or administer the activities. Key Staff designated by the Vendor will be approved by CHFS.

In addition, the Vendor should provide qualified, highly skilled project staff. The composition of the project staff should be at the Vendor's discretion. However, the Vendor should ensure that project staff meet and retain the performance standards defined in the Project Plan (Deliverable 1.1 and 1.2).

The CHFS Program Director works closely with the Vendor's Project Manager on day-to-day project activities. The Vendor should have full responsibility for providing adequate staff to complete the project in the required timeframe.

Section 30.060.030.010—Staffing Plan

The selected Vendor submits a plan for Project Staffing prior to the commencement of any work, to be approved by CHFS. The Staffing plan should describe the selected Vendor's staffing approach and team organizational structure for the prime Vendor, and all subcontracted Vendors, to complete all phases of work, functions, requirements, roles, and duties associated with this Project. The Vendor must maintain staffing levels throughout the project at ninety percent (90%) or more of the staffing plan agreed to during project planning. All MEMS Vendor staff in key roles should have recent (in the last three years) experience with implementing and/or supporting Medicaid systems.

The Project Staffing Plan includes resumes for each of the selected Vendor's proposed staffing choices for the Key Roles described below:

1. Program Manager: Primary point of contact with MEMS's Program Director for activities related to contract administration, project management, scheduling, correspondence with MEMS staff, and deliverable reviews. Should have a

Bachelor's Degree, a current Project Management Professional (PMP) Certification, and at least ten (10) years of management experience.

2. Project Manager: Responsible for planning, directing, managing and overseeing the overall Vendor Project Management activities. The primary focus is on providing an integrated view of all project and related program activities. Should have a Bachelor's Degree, a current Project Management Professional (PMP) Certification, and at least five (5) years of management experience.

3. Deputy Project Manager/PMO Manager: Also responsible for planning, directing, managing and overseeing day-to-day Vendor PMO and Project Management activities. The primary focus is on providing an integrated view of all project and related program activities. Should have a Bachelor's Degree, and at least three (3) years of management experience.

4. Core Medicaid Enterprise Systems: Primary point of contact with MEMS Technical Staff. Should serve as the Technical SME over the selected Vendor's team. Should have a Bachelor's Degree and at least seven (7) years of similar experience.

5. Systems Development Manager for DDI: Responsible for the overall functional design of all system components, functional procedures, program applications, and functional documentation. Also responsible for liaising with business SMEs on any functional decisions. Should have similar experience in MEMS Solution Development of similar size and complexity. Should have a Bachelor's Degree and at least seven (7) years of similar experience.

6. System and Web Architect: Responsible for the design, maintenance, procedures, and architecture related to data, program applications, and systems documentation. Should have similar experience in MEMS Solution Development of similar size and complexity. Should have a Bachelor's Degree and at least seven (7) years of similar experience.

7. Systems Integration Manager: Manages the integration of MEMS System Components. The number of System Manager positions corresponds to the number of MMIS modules/contracts.

    Potential Positions:

    i. Core System Project Manager
    ii. DSS Project Manager
    iii. Care Management Project Manager
    iv. Utilization Management Project Manager

    System Project Managers (PMs) are accountable for all the MEMS-related activities, reviewing and ensuring that all contractual terms and deliverables are met throughout the project and communicating project-level PM information to the Program Director.

8. Implementation Manager: Primary point of contact with Commonwealth staff regarding system implementation. Should have a Bachelor's Degree and at least five (5) years of similar experience.

9. Help Desk Manager: Responsible for internal staff User Support and Contact Center Help Desk operation. Should have a Bachelor's Degree and at least five (5) years of similar experience.

10. Operations and Maintenance Manager: Responsible for system operations and ongoing maintenance after implementation. Should have a Bachelor's Degree and at least five (5) years of similar experience.

11. Data Conversion Manager: Responsible for overall data architecture of the system including Master Data Management planning and implementation, data exchange planning and implementation and data migration to new system. Should have a Bachelor's Degree and at least five (5) years of similar experience.

12. Quality Assurance Manager: Responsible for the Vendor's implementation of their Quality Plan. Performs audits and reviews identifying areas for improvement. Should have a Bachelor's Degree and at least five (5) years of relevant experience.

The selected Vendor provides an Organizational Chart that should account for all Key Roles as well as the Lead roles listed below.

Lead roles should be filled by selected Vendor staff with appropriate levels of experience.

1. System Test Lead: Responsible for overall effort involved in system testing, including test strategy, planning, execution and status reporting. Should have a Bachelor's Degree and at least seven (7) years of similar experience.

2. Training Lead: Responsible for overall effort involved in end-user training, including training strategy, schedule, planning, training materials, delivery and status reporting. Should have a Bachelor's Degree and at least seven (7) years of similar experience.

3. Organizational Change Lead: Responsible for the creation, implementation and coordination of the Business Process Transition strategy and plan for the MEMS. Should have a Bachelor's Degree and at least five (5) years of similar experience.

4. Infrastructure Lead: Responsible for the assessment, planning, procurement, installation, configuration, maintenance and monitoring of all infrastructure components required for the MEMS. Responsible for the MEMSs server, network

and data center operations for all environments including test, production, and disaster recovery sites. Should have a Bachelor's Degree and at least five (5) years of similar experience.

5. Security Lead: Responsible for the assessment, planning and implementation of all security standards, practices and components required for the MEMS. Responsible for adherence to CHFS security standards, communications with CHFS ISO, compliance with HIPAA requirements, and IRS Federal Tax Information. Should have a Bachelor's Degree, CISM, GIAC or CISSP certification and at least five (5) years of similar experience.

6. Application Development Lead: Responsible for the planning, coordinating, and supervising of all activities related to system design and development. Should have a Bachelor's Degree and at least seven (7) years of similar experience.

7. Technical and Business Writing Quality Assurance Lead: Responsible for providing standards to be adhered to for technical and business documents and all deliverables. Responsible for enforcing and tracking compliance with quality standards and procedures including peer review processes, quality checks and remediation actions. Should have five (5) years experience in technical and business writing.

Other key positions that should be provided by the Vendor include the following:

1. Fiscal Agent Manager.
2. A minimum of one Business Analyst for each of the business areas
3. DSS Systems Engineers for ad hoc reporting.
4. Financial staff.
5. Third Party Liability staff.
6. Provider Relations representatives.
7. Provider Call Center staff.
8. EDI Staff (including EDI call center).

Modifications, Changes and Maintenance Staffing

CHFS is requiring 25,000 hours of Vendor categorized staff time per contract year to apply towards system modification, changes and enhancements to the MEMS once the system has been fully implemented for the life of the contract. Vendor should analyze the change request, provide an estimate to CHFS and receive approval prior to expending any of these hours. Any hours remaining at the end of a contract year will be rolled over to the next year. The Vendor is responsible for full-time staff support comprised of professional systems engineers (programmer/analysts) for all system maintenance change categories. This staff should be in addition to Vendor staff performing routine and general system maintenance activities. The Vendor should identify staff to be assigned to system modification, change and enhancement projects. Additionally, the staff can be assigned to support routine and general maintenance activities with the approval of the CHFS.

Other non-programming categorized staff should support routine and general maintenance activities that include: workflow analysis, system testing, documentation updates, and program procedure activities may consist of architects, testers, business analysts, security experts, Database Analysts (DBAs), change management personnel, and/or administrative staff. The mix should be left up to the Vendor, as long as the required level of service is met.

Vendor staff responsibilities for all system maintenance activities are prioritized by the CHFS, with input from the Vendor. Within these priorities, the Systems Manager is responsible for directing the work of Vendor staff to ensure that all maintenance and modification efforts proceed in a timely manner. All module and system component functions should be covered by at least one Vendor systems/programming staff with extensive knowledge and experience in the corresponding technical area. Team members should be sufficiently cross-trained to support temporary changes in priorities and/or responsibilities.

The selected Vendor should explain in its Staffing Plan how each individual meets the requirements of the proposed role. All proposed Vendor staffing for Key Roles is subject to approval by CHFS. CHFS reserves the right to reject the Vendor's proposed individuals for Key Roles. In such a case the selected Vendor should be required to provide an alternative staffing proposal for that Key Role. CHFS reserves the right to interview individuals proposed to Key Roles, if desired, prior to approval of any staffing.

CHFS and its stakeholders should be interacting with the selected Vendor's staff on an ongoing basis, and as such the selected Vendor should submit in its plan an organizational chart for Staffing that describes how the selected Vendor's team should interact with CHFS staff and key Commonwealth stakeholders.

In addition, the selected Vendor may need to interact with other Vendors associated with the delivery of the MEMS including the IV&V Vendor. The selected Vendor should cooperate with all resources involved in the MEMS project to ensure the successful integration of all components of the solution and the overall delivery of operationally efficient and effective MEMS.

CHFS recognizes that changes in the selected Vendor's level of Staffing may happen due to a variety of unforeseen factors. However, the selected Vendor is responsible for ensuring the appropriate experienced staffing level is maintained throughout the project to ensure the objectives of this Project are met on time.

To mitigate risks associated with changes in Vendor staffing, CHFS requires the selected Vendor to include a contingency plan with the Project Staffing Plan. The contingency plan should address staffing changes to include: replacement of key personnel or other proposed staff, staff augmentation plans in the event of an inability to meet performance standards, and a method for deploying and bringing new team members up to date with the project.

Section 30.060.030.020—Onsite Staffing Requirement

During the DDI Phase, CHFS will provide space for Vendor staff onsite in Frankfort, KY. This includes the following Key Vendor staff:

1. Program Manager, as required.
2. Project Manager (at least 80% of the time).
3. Deputy Project Manager (100% commitment).
4. Project Management Office (PMO) Manager (100% commitment).
5. Core Medicaid Enterprise Systems Manager (100% commitment).
6. Systems Development Manager for Design and Development (100% commitment).
7. Systems Integration Manager (100% commitment).
8. Implementation Manager (100% commitment).
9. Data Conversion Manager (100% commitment)
10. Quality Assurance Manager (100% commitment).

The Commonwealth and Key Vendor staff should work very closely together on this project. This requires an onsite presence. It is vital for the Vendor project manager and key staff to play an active role in the project and be visible and accessible.

Once the new MEMS are implemented, the key technical staff should continue to be housed at the CHFS facility throughout five year operational period. These staff include:

1. Core Medicaid Enterprise Systems Manager.
2. System Analysts/Engineers.
3. Network staff.
4. Configuration Manager
5. DSS Systems Engineer for maintenance.
6. Privacy/Security Compliance Management.

The key FA staff should be located in a Vendor supported facility within twenty (20) miles of the Kentucky Department of Human Resources Building. Staff that should be located there are:

1. Fiscal Agent Manager.
2. A minimum of one Business Analyst for each of the business areas
3. DSS Systems Engineers for ad hoc reporting.
4. Financial staff.
5. Third Party Liability staff.
6. Provider Relations representatives.
7. Provider Call Center (some in Frankfort; can have additional sites).
8. EDI Staff (including EDI call center).
9. Trainers.

Section 30.060.030.030—Offsite Project Work

The Commonwealth will permit development project work to be performed offsite. For offsite work, the Commonwealth requires strong management of the resources and

assigned activities; adequate, timely and accurate communications and completion of assigned work by specified deadlines. This is important to any offsite relationship.

Section 30.060.040—Systems Development Life Cycle Methodology (Section 60.010.010.060)

Prior to the commencement of work, the selected Vendor should submit a description of the SDLC Methodology that it plans to use for the MEMS, for review, comment, and approval by CHFS.

The selected Vendor should deliver the solution using a phased development approach that supports the Commonwealth's requirement to review and test iterations of development of logical functional groups of system components, before proceeding to the System Test phase. Therefore, the plan for the Development Phase should account for durations of Commonwealth testing and feedback, and system updates by the Vendor, prior to the completion of the Development phase for each iteration.

Section 30.060.050—Project Deliverables and Milestones (Section 60.010.010.060)

For each project deliverable, a required minimum specification has been defined and is included in Appendix G – Deliverables. All deliverables should be delivered and maintained online in the SharePoint Project Repository that is required in Activity 1 (Deliverable 1.5). The SharePoint Project Repository is the central location for the delivery, management and maintenance of all artifacts of the Project, including all deliverables. CHFS will provide an area on its SharePoint portal for the Vendor to organize and utilize for its repository. The CHFS Project Team should have continuous access to the SharePoint Project Repository to review and accept deliverables and to provide ongoing management of the project. The schedule for the submission of deliverables should be based on the Vendor's approved Project Plan.

In the process of developing deliverables, the Vendor should involve the CHFS Project Team and the IV&V Vendor in a review of a draft version of the deliverable. Prior to submission of the draft document, the Vendor's review process should incorporate the Vendor's Internal Quality Management review steps described in the Vendor's Project Plan. As each deliverable is formally submitted, the Vendor should provide evidence to show that the Vendor's review and corrective action has been followed through the versioning process.

All deliverables should be delivered to the CHFS Program Director. A cover letter should be included with an electronic copy of the Deliverable and placed on the SharePoint Project Repository in a specified area. Additional versions may be required by CHFS in different formats.

Upon receipt of a deliverable, CHFS will log the deliverable and convene a review panel to initiate the review process. CHFS will simultaneously provide Contract deliverables to the IV&V Vendor for its independent review. As necessary, the Vendor may be asked to provide a walk-through of each deliverable to aid the review panel and the IV&V Vendor in understanding the document. CHFS and the IV&V Vendor should review deliverables

to determine their readiness for use and compliance with content requirements specified in Appendix G – Deliverables. CHFS will complete its review and provide review results in writing to the Vendor within 15 days. If CHFS finds deficiencies in deliverables, it will formally communicate them in writing to the Vendor. The Vendor should correct deficiencies and resubmit corrected deliverables for review within 10 days from receipt of CHFS notification of deficiencies (which begins a new 15-day CHFS review cycle). Deliverables must be approved in writing by CHFS to be considered final.

The table below provides a summary list of all the required deliverables. The table indicates the Activity number and description and the Deliverable number and description.

Table 1 – Summary of Deliverables

Activity	Activity Description	Deliverable Number	Deliverable
1	Project Management		
		1.1	Project Plan
		1.2	Project Plan Updates
		1.3	Configuration Management Plan
		1.4	Software Development Methodology
		1.5	SharePoint Project Repository
		1.6	Project Status Reports
		1.7	Security Policies and Procedures
		1.8	Business Continuity Plan – V1: Development
2	Detailed Requirements Analysis		
		2.1	Detailed Requirements (RSD)
		2.2	General System Design (GSD)
3	Design		
		3.1	Detailed System Design (DSD) Version 1
		3.2	Implementation Plan – Version 1
		3.3	System Architecture and Design Documents a) Interface Detail Design (IDD) and Integration Specification document b) Interface Control Document (ICD)
		3.4	Architectural Review Board
		3.5	Test Management Plan
		3.6	Network Upgrade Requirement
		3.7	Data Conversion Strategy
4	Development		
		4.1	Development Environment*
		4.2	Code Library – Version 1: Test Environment*

Activity	Activity Description	Deliverable Number	Deliverable
		4.3	Development Test Results*
		4.4	User Manual – Version 1*
		4.5	Operating Procedures – Version 1*
		4.6	Detailed System Design Version 2
5	Data Conversion		
		5.1	Data Conversion Plan
		5.2	Conversion Test Results*
6	Business Process Transition		
		6.1	Comprehensive Behavior Process Transition and Communication Plan
		6.2	BPR Modeling of Future Processes
		6.3	Training of Staff on New Processes
		6.4	New Process Rollout
		6.5	BPR Results Report
7	Acceptance Testing		
		7.1	Test Environment*
		7.2	Acceptance Test Plan*
		7.3	Acceptance Test Results*
		7.4	Operational Test Plan*
		7.5	Operational Acceptance Test Results*
		7.6	Source Code Library – Version 2: Acceptance Testing Environment*
		7.7	Business Continuity Plan for Systems Operations and Maintenance
		7.8	Detailed System Design Version 2
8	Training	8.1	Training Strategy*
		8.2	Training Plan*
		8.3	Training Environment*
		8.4	Training Materials*
		8.5	Training Report*
9	Implementation		
		9.1	Implementation Plan – Version 3*
		9.2	Production Environment*
		9.3	Source Code Library – Version 3: Production Environment*
		9.4	User Manual – Version 2
		9.5	Operating Procedures – Version 2*
		9.6	Detailed System Design Version 3 (Sysdoc)

Activity	Activity Description	Deliverable Number	Deliverable
		9.7	Implementation Certification Letter
10	Operations		
		10.1	Quality Management Plan
		10.2	Staffing Requirements Capability Report
		10.3	Bi-weekly Status Report for Operations
		10.4	Annual Status Report for Operations
11	Certification		
		11.1	Certification Checklist
		11.2	Certification Review Package
12	Systems Operation and Maintenance Support		
		12.1	Systems Support Plan
		12.2	Staffing Requirements Capability Report
		12.3	Biweekly Status Report
		12.4	Annual Status Report
		12.5	System Updates
		12.6	Operations & Maintenance Procedures Manual
13	Turnover		
		13.1	Turnover Plan
		13.2	Requirements Statement
		13.3	Systems Documentation
		13.4	Source Code Library
		13.5	Turnover Results Report

Deliverables noted with an asterisk (*) should be approved prior to commencement of other systems development activities.

The activities/deliverables above are assigned to milestones in the table below as follows:

Table 2 – Milestones, Activities and Deliverables

Milestone	Activity Description	Deliverable
Design	Project Management	
		Project Plan
		Project Plan Updates
		Configuration Management Plan
		Software Development Methodology
		SharePoint Project Repository
		Project Status Reports

Milestone	Activity Description	Deliverable
		Security Policies and Procedures
		Business Continuity Plan – V1: Development
Design	Detailed Requirements Analysis	
		Detailed Requirements (RSD)
Design	Design	
		Detailed System Design (DSD) Version 1
		Implementation Plan – Version 1
		System Architecture and Design Documents a) Interface Detail Design (IDD) and Integration Specification document b) Interface Control Document (ICD)
		Architectural Review Board
		Test Management Plan
		Network Upgrade Requirement
		Data Conversion Strategy
Development/Testing	Development	
		Development Environment*
		Code Library – Version 1: Test Environment*
		Development Test Results*
		User Manual – Version 1*
		Operating Procedures – Version 1*
		Detailed System Design Version 2
Conversion	Data Conversion	
		Data Conversion Plan
		Conversion Test Results*
Acceptance Testing	Acceptance Testing	
		Test Environment*
		Acceptance Test Plan*
		Acceptance Test Results*
		Operational Test Plan*
		Operational Acceptance Test Results*
		Source Code Library – Version 2: Acceptance Testing Environment*
		Business Continuity Plan for Systems Operations and Maintenance
		Detailed System Design Version 2
Implementation	Implementation	
		Implementation Plan – Version 3*
		Production Environment*

Milestone	Activity Description	Deliverable
		Source Code Library – Version 3: Production Environment*
		User Manual – Version 2
		Operating Procedures – Version 2*
		Detailed System Design Version 3 (Sysdoc)
		Implementation Certification Letter
Certification	Certification	
		Certification Checklist
		Certification Review Package

Deliverables noted with an asterisk (*) should be approved prior to commencement of other systems development activities.

Section 30.060.060—Facilities and Equipment

During the DDI phases, the Vendor's project team will be provided space at the Commonwealth. It has been CHFS's experience that having the Vendor and Commonwealth project teams housed together facilitates more open communication and lends itself to a more successful project. Following the MEMS implementation, key technical staff should remain housed with CHFS in its support of the system operations, maintenance, and modifications.

Commencing with the FA operations phase, the Vendor will maintain its facility in Kentucky within a radius of 20 miles from the Frankfort, Kentucky Department of Human Resources Building, located at 275 East Main Street, with access for designated CHFS staff. The Vendor will provide access 24x7x365 to all Vendor Medicaid Enterprise facilities and operations in Kentucky and to each Medicaid employee designated by the Commonwealth, without prior notice, admission, escort, or other requirements. All Vendor and Commonwealth staff and visitors should wear identification badges at all times while in the facility. The Commonwealth and the Vendor will establish appropriate protocols to ensure that physical property/facility security and data confidentiality safeguards are maintained. Access to any non-Kentucky facility used to support the Medicaid Enterprise will be granted within five workdays of the request.

Section 30.060.070—Activity 1 – Project Management (Section 60.010.010.060)

This Section presents the requirements for Project Management to be completed over the Contract period for Activities 1 through 13. Project Management activities span the duration of the Project. Project Management activities that support the use of the Project Plan are the primary control elements on the Project.

Section 30.060.070.010—Objectives

The specific objectives of the Project Management Activity are to ensure that the MEMS meets Kentucky's specific requirements defined in Appendix A – MEMS Functional Requirements, Appendix B – MEMS Technical Requirements, and the current CMS

functional equivalency and reporting requirements identified in the State Medicaid Manual (SMM), Part 11.

The Project Management Activities are designed to ensure that the Project progresses according to the approved detailed Project Plan. The activities and associated activities related to Project management are in the following sections. The Vendor's project methodology should align within the Commonwealth's overall project management framework.

The Vendor should develop an initial Project Plan with CHFS input within 20 days of Project initiation. Once the Project Plan is approved by CHFS, the approved Project Plan should be maintained by the Vendor. The Vendor should modify the Project Plan throughout the Project, with CHFS approval, by updating it to reflect the evolving schedule, priorities, and resources.

As part of the Project Management Activity, the Vendor should also provide documentation of systems development processes and controls to be used to ensure a quality MEMS development and implementation. The documentation of processes and controls should include a Software Development Plan, Security Policies and Procedures, and the Business Continuity Plan. An implementation plan is to be included in the Project Plan as well.

CHFS will provide an area on its SharePoint portal for the Vendor's use. The Vendor should organize this SharePoint Project Repository which should provide access to all Contract Deliverables. The CHFS Project Team will have continual access to the SharePoint Project Repository.

Section 30.060.070.020—CHFS Project Management Responsibilities

CHFS Project Management responsibilities in this activity are to:

1. Manage the MEMS Project Risk Management Plan and process including periodic input from the Vendor and the IV&V Vendor.
2. Conduct periodic meetings of the MEMS Requirements Management Change Control Board (CCB) in order to manage project change requests.

Section 30.060.070.030—Vendor Project Management Responsibilities

Vendor Project Management responsibilities are to:

1. Prepare, submit, gain approval, and execute the Project Plan as defined in Appendix G – Deliverables (Deliverables 1.1 & 1.2). The Vendor must obtain CHFS approval of the Project Plan before commencing work on the activity. The Vendor should submit updates to the Project Plan monthly, at a minimum.
2. Maintain staffing levels throughout the project at ninety percent (90%) or more of the staffing plan agreed to during project planning.
3. Present the Software Development Plan and the Change Management Plan to the CHFS Project Team. Utilize the plans during project execution.
4. Prepare and submit Project Status Reports. The Status Reports should be in the format approved by CHFS and include accomplishments, critical issues, personnel utilized, and items planned for the next reporting period. The Status

Reports should report identified issues and risks and associated mitigation strategies in support of the MEMS Project Risk Management Plan. The Status Reports should conform to the requirements described in Appendix G – Deliverables and should be presented to the CHFS Program Director and the IV&V Vendor weekly.

5. Establish and begin using the approved SharePoint Project Repository (Deliverable 1.5) as the control system for all Project Deliverables and other artifacts. Deliverables are expected to be delivered, managed, and controlled through the SharePoint Project Repository.
6. Participate in the MEMS Requirements Management Change Control Board (CCB) as needed.
7. Develop, submit, and utilize the Security Policies and Procedures in Appendix G – Deliverables (Deliverable 1.7) and the Business Continuity Plan in Appendix G – Deliverables (Deliverable 1.8).
8. Attend meetings and present Project status as directed by the CHFS Program Director.
9. Support the IV&V process as defined in RFP.
10. Prepare and submit final deliverables.

Section 30.060.070.040—Milestones

The critical milestones that affect the schedule or impact progress during the Project Management activity are:

1. CHFS approval of the Project Plan deliverables and the Software Development Plan deliverable.
2. CHFS approval of the SharePoint Project Repository deliverable.
3. CHFS approval of the Security Policies and Procedures deliverable and the Business Continuity Plan deliverable.
4. CHFS approval of monthly Project Plan updates.
5. CHFS approval of weekly Status Reports.

Section 30.060.070.050—Deliverables

This section defines the Vendor deliverables related to the Project Management Activity. Preparation, maintenance, and use of quality deliverables are critical to the success of the Project Management process and should be used to assess the Vendor's overall understanding of requirements and expectations of CHFS. Documents prepared during the Project Management Activity are the foundation for the definition of work to be completed in subsequent Project activities. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables. The deliverables to be provided during the Project Management activity are:

Table 3 – Activity 1 Deliverables

NUMBER	DELIVERABLE	SECTION
1.1	Project Plan*	G.1.1
1.2	Project Plan Updates	G.1.1

NUMBER	DELIVERABLE	SECTION
1.3	Configuration/Change Management Plan	G.1.2
1.4	Software Development Methodology*	G.1.3
1.5	SharePoint Project Repository Organization	G.1.4
1.6	Project Status Reports	G.1.5
1.7	Security Policy and Procedures	G.1.6
1.8	Business Continuity Plan – Version 1: Development	G.1 .7

Deliverables noted with an asterisk (*) should be approved prior to commencement of other systems development activities.

CHFS review of the Services and Deliverables of this activity should ensure that:

1. The Project is managed on schedule, within scope, and within budget.
2. Integrated plans are established and maintained to coordinate a comprehensive list of activities and tasks to handle the breadth of system requirements and the involvement of a large number of MEMS stakeholders.
3. Facilities and equipment are procured and established or installed.
4. Integrated plans are established to ensure quality systems development processes are in place to create quality system components.
5. An infrastructure is established to assure that the development, testing, training, and production environments are adequately secure to protect MEMS and data.
6. The SharePoint Project Repository is the means of access and review of MEMS documentation during development and maintenance.
7. Communications are established and maintained that provide adequate progress reporting, problem and risk identification and resolution and Contract management information.
8. The development process allows for internal Vendor quality processes and external independent Quality Assurance activities.
9. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.080—Activity 2 – Detailed Requirements Analysis

The Detailed Requirements Analysis Activity requires analyzing, defining, and further developing business, technical and functional requirements that are included in the base system for the new MEMS. The requirements should be further refined to arrive at the detailed design requirements that should be traced throughout the DDI process via the Requirement Traceability Matrix (RTM) and to the requirements specified in the RFP (Appendix G – Deliverables).

The products of this analysis should serve as the foundation for Detailed System Design documents and the draft version of the System Architecture and Design that is generated in Activity 4. The Requirements Analysis documentation becomes the initial version of the System documentation and should be updated as subsequent activities are completed.

Section 30.060.080.010—Objectives

The objective of this activity is to validate and finalize the requirements for this Project. The outcome of this activity is a requirements baseline that should be reviewed and revised throughout the change management process on a continuing basis as requirements are addressed. The Vendor is required to identify and document the system business rules to be supported by the new MEMS. This activity includes the on-going management of the requirements identified in this activity.

Section 30.060.080.020—CHFS Detailed Requirements Analysis Responsibilities

CHFS responsibilities for the Detailed Requirements (Functional and Technical) Analysis activity are:

1. Provide an Implementation Team of full-time individuals with duties that include working with the Vendor to help design the MEMS during the Design Phase.
2. Participate in Joint Application Design (JAD) sessions to assist the Vendor in understanding the CHFS role, Vendor role, and requirements for each business function.
3. Review all prototypes, window designs, architecture designs, work plans, requirements documents, and all deliverables and provide quick response and comment.
4. Monitor the MEMS Requirements Management process and conduct MEMS Requirements Change Control Board Meetings as needed.

Section 30.060.080.030—Vendor Detailed Requirements Analysis Responsibilities

Vendor responsibilities for the Detailed Requirements Analysis activity are:

1. Perform a detailed review and analysis of all requirements provided in the RFP and should develop the detailed specifications required to construct and implement the MEMS solution. The Vendor should thoroughly review all appropriate Kentucky Medicaid programs and policies and legacy MMIS documentation. The Vendor should work with CHFS staff to fully understand the scope, purpose, and implications of each requirement.
2. Plan and conduct JAD sessions, whose form, structure, timeframe, and schedule are prior approved by the CHFS.
3. Validate and refine the requirements specified in this RFP with CHFS staff.
4. Verify that the capabilities described in the Vendor proposal actually align with and meet the RFP requirements.
5. Validate that the capabilities described in the Vendor proposal meet MITA requirements.
6. Document the purpose and results of each JAD session.
7. Produce agendas and subject matter expert (SME) rosters for approval by the CHFS prior to distribution.
8. Prepare session minutes for approval by the CHFS prior to distribution.
9. Document Use Cases.
10. Document and track all action items during sessions through the project management portal.

11. Document the rules in the existing legacy system as appropriate for incorporation into the new MEMS rules engines including benefit plan assignment, pricing rules, and the edit and audit rules.
12. Elaborate and document architectural, and business and technical functional requirements described in this RFP and in attachments for the new MEMS.
13. Document and model each business process.
14. Develop acceptance criteria. This measurement should be used to generate the necessary test cases for system and acceptance testing.
15. Support and participate in requirements management.
16. Construct and update the Requirements Traceability Matrix (RTM).
17. Document the requirements validation.
18. Participate with the CHFS Requirements Change Control Board and process as needed.
19. Support the IV&V process as defined in the RFP.
20. Prepare and submit final Deliverables for approval.

Section 30.060.080.040—Milestones

The critical milestones that affect the schedule or impact progress during the Detailed Requirements Analysis (both Functional and Technical) activity are:

1. Complete the review of documentation pertaining to the legacy MMIS and related processes.
2. Complete the review of business, system, and user requirements documented by CHFS.
3. Complete the detailed requirements analysis meetings with appropriate CHFS staff. This activity should be done in parallel with the workflow and process engineering activities in Activity 3. Prepare the requirements baseline document and completion of walk-through with appropriate CHFS staff.
4. Prepare updated requirements documentation reflecting CHFS comments.
5. Obtain CHFS approval of the Detailed Requirements Document (DRD) deliverable.

Section 30.060.080.050—Deliverables

This section defines the Vendor Deliverables related to the Detailed Requirements Analysis (both Functional and Technical) Activity. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 4 – Activity 2 Deliverables

NUMBER	DELIVERABLE	SECTION
2.1	Detailed Requirements – Requirements System Design*	G.2.1
2.2	General System Design	G.2.2

Deliverables noted with an asterisk (*) should be approved prior to commencement of other systems development activities.

CHFS' review of the Services and Deliverables of this activity should ensure that:

1. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.090—Activity 3 – Design

The goal of the Design Activity is to develop the logical architecture of the system and support development of detailed programming specifications. Design activities should be consistent with the technical approach presented in the Vendor's Detailed Requirements Analysis.

Implementation plans should be developed during the Design Activity to clearly articulate *who* should be responsible, *what* are the various activities involved, and *how* they are to be delivered on time and on budget to meet project expectations. More importantly, the plan should explicitly identify and address implementation challenges and risks and be updated concurrently with each project phase as the project evolves.

Early in the Design Activity, the number and scope of test plans should also be determined and be approved by the CHFS prior to the start of testing. As applicable, test scenarios, test scripts, and test cases within each phase of testing should align with the Requirements Traceability Matrix (RTM) to verify all requirements are accounted for. Successful test results should confirm all requirements have been thoroughly tested.

Section 30.060.090.010—Objectives

The objective of the Design Activity is to define the blueprints for the new MEMS. Utilizing the detailed requirements deliverable, the Vendor should identify, change if necessary, obtain DMS approval, and finalize the business and technical functional requirements in a design document for the MEMS. The design should be used by programming staff to further analyze and construct the services for the new MEMS. The Vendor should be responsible for presenting changes to model prototypes for CHFS staff to review throughout the design process. The Vendor should be responsible for conducting a walk-through of the Detailed System Design (DSD) with CHFS to enhance CHFS's understanding and to facilitate the approval process. Application Programming Interfaces (APIs) used to communicate between components and modules or with external systems should also be defined in the DSD document.

Implementation planning has a strong management focus which requires best practice approaches, skills and experience. The Vendor should prepare an implementation plan (Deliverables 3.2, 4.7, 9.1) to execute its implementation strategy for successful deployment of the MEMS on schedule, on scope and on budget.

The Vendor should complete the Architecture Review Board (ARB) (Deliverable 3.4) requirement and CHFS must approve the deliverable documents in order to complete the Design Phase. Portions of the DSD approved by CHFS may be used to satisfy ARB standards and deliverable requirements. The Vendor should also include a preliminary system network architecture draft diagram for each proposed environment in the proposal until architecture diagrams can be finalized.

The Vendor should prepare a Test Management Plan (Deliverable 3.5) to ensure all requirements are addressed and system modules, system components, and system interfaces operate as designed within the MEMS SOA framework including:

1. Modules are integrated using the defined technology and follow the prescribed method of governance.
2. Medicaid business rules perform as documented.
3. Business modules perform as described in the design phase.
4. The MEMS performs as expected during load and stress testing.
5. A safe environment is available for users to test the system.
6. All tests have been completed, documented, and passed by the Commonwealth, and interfaces comply with the Interface Control Document (ICD).

The Vendor should prepare a Data Conversion Strategy (Deliverable 3.7) to be delivered as part of the proposal for which its primary purpose is to document and communicate the data conversion scope, objectives, approach, and requirements.

Section 30.060.090.020—CHFS Design Responsibilities

CHFS responsibilities for the Design activity are:

1. Modify the CHFS network and desktops to meet the requirements using the Network Upgrade Requirements Deliverable.

Section 30.060.090.030—Vendor Design Responsibilities

Vendor responsibilities for the Design activity are:

1. Prepare the Detailed System Design document.
2. Prepare the Implementation Plan (Version 1.0).
3. Prepare the System Architecture and Design document.
4. Prepare the Architectural Review Board documents.
5. Prepare the Test Management Plan.
6. Prepare the Network Upgrade Requirements Deliverable.
7. Prepare the Date Conversion Strategy Document.
8. Support the IV&V process as defined in the RFP.
9. Prepare and submit Deliverables for approval.

Section 30.060.090.040—Milestones

The critical milestones that affect the schedule or impact progress during the Design activity are:

1. Preparation of the DSD document and draft System Architecture and Design document and walk-through with appropriate CHFS staff.
2. CHFS approval of the DSD and System Architecture and Design documents.
3. CHFS approval of the Architectural Review Board documents.
4. Completion and CHFS approval of the Implementation Plan (version 1.0) and the Test Management Plan.

5. Completion and CHFS approval of the Network Upgrade Requirements Deliverable.
6. Completion and CHFS approval of the Data Conversion Strategy document.

Section 30.060.090.050—Deliverables

The table below identifies the Deliverable number and description and the section where further information can be found in Appendix G – Deliverables. The Vendor should meet the requirements for Deliverables presented in Appendix G – Deliverables:

Table 5 - Activity 3 Deliverables

NUMBER	DELIVERABLE	SECTION
3.1	Detailed System Design Version 1	G.3.1
3.2	Implementation Plan – Version 1	G.3.2
3.3	System Architecture and Design Documents (SADD) a) Interface Detail Design (IDD) and Integration Specification document b) Interface Control Document (ICD)	G.3.3
3.4	Architectural Review Board	G.3.4
3.5	Test Management Plan	G.3.5
3.6	Network Upgrade Requirement	G.3.6
3.7	Data Conversion Strategy	G.3.7

CHFS review of the Services and Deliverables of this activity should ensure that:

1. The DSDs correlate and accurately reflect business processes and workflows and technical function requirements.
2. The System Architecture and Design addresses the defined functional, performance and security requirements of the system and assures the required data interfaces with other systems.
3. The Architectural Review Board documents are in compliance with CHFS standards and are compatible with the CHFS Enterprise architectural framework.
4. The Systems design is compatible with the CHFS network/computing environment and with the network upgrade requirements, should adequately meet the MEMS requirements.
5. The implementation plan is iteratively developed to identify additional risks and issues while executing the defined scope and schedule of the plan.
6. The Testing Plan allows CHFS to track testing of the MEMS during development, and deliverables meet the minimum requirements defined in Appendix G – Deliverables.
7. The data migration strategy used to transfer system data from the legacy MMIS to the new MEMS provides a sustainable roadmap yielding complete, accurate, successful results.

Section 30.060.100—Activity 4 – Development

This activity addresses system development activities related to the new modular MEMS that complies with all of the requirements of this RFP. The Vendor should ensure that development is based on the CHFS-approved DSDs and System Architecture and Design and complies with all current State and Federal requirements.

Section 30.060.100.010—Objectives

The major objectives for this activity are the development and testing of the new MEMS to achieve the functional and technical requirements established during activity 2, the Detailed Requirements Analysis and Design Activities. Development and testing work should be completed according to the CHFS approved Implementation Plan.

It is important to point out that those areas where the system may not meet the functional requirement in its entirety that a decision needs to be made as to which is more efficient; to align the business process with the standard or the system. This is part of the construction process and should also tie into Activity 6.

Section 30.060.100.020—CHFS Development Responsibilities

CHFS responsibilities for the development activity are:

1. Facilitate the testing processes by providing test data and test files to the Vendor.
2. Perform testing activities.

Section 30.060.100.030—Vendor Development Responsibilities

Vendor responsibilities for the Development activity are:

1. Provide the Development Environment that consists of the system hardware, software, networks and workstations to develop and implement the new MEMS.
2. Execute and report on planned development activities.
3. Develop the Test Plan that consists of the plans to conduct unit, system, integration, stress and acceptance testing.
4. Develop MEMS documentation including the User's Manual – Version 1 and Operating Procedures – Version 1.
5. Complete Test Plans and conduct testing as planned.
6. Support the IV&V process as defined in RFP.
7. Document test results.
8. Conduct walk-through of Deliverables as needed.
9. Prepare and submit Deliverables for approval.

Section 30.060.100.040—Milestones

The critical milestones that affect the schedule or impact progress during the Development activity are:

1. CHFS acceptance of the development environment.
2. Completion of unit, system, integration, stress and acceptance testing.
3. CHFS approval of test plan and Development Test Results.

4. CHFS approval of new and updated systems documentation (e.g., User Manual, Operating Procedures, DSDs) and code library deliverables.
5. Walk-through of draft deliverables.

Section 30.060.100.050—Deliverables

This section defines the Vendor Deliverables related to the Development Activity of the Project. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 6- Activity 4 Deliverables

NUMBER	DELIVERABLE	SECTION
4.1	Development Environment*	G.4.1
4.2	Code Library – Version 1: Test Environment*	G.4.2
4.3	Development Test Results*	G.4.3
4.4	User Manual – Version 1*	G.4.4
4.5	Operating Procedures – Version 1*	G.4.5
4.6	Detailed System Design Version 2	G.4.6
4.7	Implementation Plan – Version 2	G.4.7

Deliverables noted with an asterisk (*) should be approved prior to commencement of the Acceptance Testing Activity.

CHFS review of the Services and Deliverables of this activity should ensure that:

1. A development environment is established that provides a mature process to support the extension of the proposed Base System to meet CHFS requirements and to support future maintenance and enhancement activities.
2. Planned development activities and methodologies are executed and reported.
3. The MEMS is developed while maintaining version control integrity.
4. MEMS error identification and closure is tracked and reported.
5. CHFS approves the MEMS for transition to the Acceptance Testing and the Training activities based on an agreement that defines the level of open system errors.
6. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.110—Activity 5 – Data Conversion (60.010.010.100)

An integral part of the project should be to integrate into the new system, historical data from the existing CHFS MMIS.

Conversion controls, especially the monitoring and proof of initial conversion results, are very important to ensure that the transactional source data converted into the system is accurate prior to implementation. Initial and ongoing conversion controls and balancing procedures should be described. The Vendor should make every effort to maintain data integrity and validity as data is converted to support the new MEMS. The Vendor should develop a plan that outlines the process to be used to ensure that the entire conversion

activity results in accurate migration of system data to the new MEMS and should execute the plan upon approval from CHFS.

Section 30.060.110.010—Objectives

The conversion process, which precedes the Implementation Activity of the Project, should be error free and completed before acceptance testing can proceed. The planning and execution of the conversion activities should be comprehensive and well documented. The new databases should be able to distinguish converted data from new data and all converted data should be date sensitive. Data mapping and conversion modules should be well documented in order to support research of conversion problems uncovered during the implementation and operations activities

Section 30.060.110.020—CHFS Conversion Responsibilities

CHFS responsibilities for the Data Conversion activity are:

1. Respond to Vendor inquiries related to data mapping, system conversion requirements, and CHFS policies and procedures.
2. Assist with resolution of Data Conversion issues.
3. Respond to Vendor inquiries related to MEMS interfaces.

Section 30.060.110.030—Vendor Data Conversion Responsibilities

Vendor responsibilities for the Data Conversion activity are:

1. Develop a Data Conversion Plan that defines:
    a. A complete list of data, files, and tables to be converted, including the sources of the data.
    b. A list of default data values and new data requirements as needed.
    c. A data mapping between current systems and the future systems and provide a conversion plan, including a description of how full conversion should be completed and validated.
2. Conduct data conversion according to the Data Conversion Plan.
3. Identify, track, and resolve data anomalies during data conversion.
4. Develop and test conversion programs.
5. Handle all required manual data conversion or data entry activities needed.
6. Prepare conversion test results document.
7. Conduct walk-through of Deliverables.
8. Obtain CHFS comments on draft Deliverables.
9. Support the IV&V process as defined in the RFP.
10. Prepare and submit final documents for approval.

Section 30.060.110.040—Milestones

The critical milestones that affect the schedule or impact progress during the Data Conversion activity are:

1. CHFS approval of Data Conversion Plan Deliverable.
2. CHFS approval of Data Conversion Testing Results Deliverable.

Section 30.060.110.050—Deliverables

This section defines the Vendor Deliverables for the Data Conversion Activity. The table below identifies the Deliverable number and description; and the section where further information can be found in Appendix G – Deliverables.

Table 7 – Activity 5 Deliverables

NUMBER	DELIVERABLE	SECTION
5.1	Data Conversion Plan	G.5.1
5.2	Conversion Test Results*	G.5.2

Deliverables noted with an asterisk (*) should be approved prior to commencement of the Acceptance Testing Activity.

CHFS review of the Services and Deliverables of this activity should ensure that:

1. The source of data is properly mapped into the new MEMS database.
2. Data anomalies are identified and closure is tracked and reported.
3. CHFS approves the System for transition to the Acceptance Testing and Training Activity based on an agreement that defines the closure of open data anomalies.
4. The accuracy of data conversion is validated.
5. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.120—Activity 6 – Organization Change Management (Section 60.010.010.080)

The purpose of the Organization Change Management activity is to successfully support DMS in the transition from the current business processes and organizational structure, to the future business practices and organizational structure surrounding the new MEMS in a controlled way. The Vendor should be expected to strive to integrate these change efforts with any ongoing CHFS-wide Organizational Change program at the time of the development effort.

Section 30.060.120.010—Objectives

The change management activity is directed at maximizing positive response to the new MEMS by effectively managing stakeholder expectations and helping to ensure smooth adoption of the new system. It incorporates effective communication and highlights impacts on affected business processes. At a minimum, the activity limits disruption of staff and minimizes impact to the Medicaid members. CHFS is looking to move forward along the MITA maturity continuum in its business processes. The Vendor should work with the Commonwealth to achieve MML increases from its current MML 1.

The Organizational Change Management Plan includes business process reengineering (BPR), which is a strategy focusing on the analysis and design of workflows and processes within an organization. BPR aims to help the organization improve its business processes in order to improve customer service, become more efficient, and potentially cut operational costs. The Vendor should accomplish the BPR goals by

completing all requirements and delivering all deliverables identified as part of the BPR tasks:

1. Assess and reengineer the business processes of the core business areas that make-up and drive the MEMS.
2. Identifying BPR objectives.
3. Identifying performance problems.
4. Demonstrate opportunities for improvements.
5. Reengineer, redesign, and model business processes.
6. Set and/or assist in setting performance improvement goals.
7. Implement reengineered business processes.
8. Train designated Medicaid staff on BPR.

Section 30.060.120.020—CHFS Organizational Change Management Responsibilities

1. Identify Commonwealth lead for management and execution of the Organizational Change Management Plan.
2. Provide direction on the organization change management strategy.
3. Collaborate on the identification of leaders and power users.
4. Collaborate on the schedule.
5. Recruit and schedule leaders and power users.
6. Execute cultural change activities as identified and agreed upon.

Section 30.060.120.030—Vendor Organizational Change Management Responsibilities

1. Plan, schedule, and conduct meetings with appropriate Commonwealth staff to collaborate on strategies for change management and communication with all stakeholders, which includes internal project staff.
2. Develop organizational change strategy and the plan for communication based on meetings and feedback from Commonwealth staff.
3. Set business process performance standards and capture baseline metrics.
4. Provide design templates and documentation on developing effective and efficient business processes.
5. Define, document, and map a complete set of business processes for all MEMS business areas to show efficiencies, logical, physical and resource transitions from the existing business processes to new business processes.
6. Create new streamlined and efficient business processes based new features and functions of MEMS.
7. Improve or create performance improvements that contribute to reducing administrative cost and promote efficient use of resources.
8. Reengineer and streamline inefficient and ineffective business processes into efficient and effective business processes, achieving dramatic improvements in performance.

9. Provide training and mentoring for Medicaid staff to a level of proficiency in the development of efficient business processes, the business processes design methodology, mapping and implementation strategies.
10. Implement reengineered business processes, monitor performance, and rework unproductive reengineered business processes.
11. Support the IV&V process as defined in the RFP.

Section 30.060.120.040—Milestones

1. Deliverable 6.1: Comprehensive Organizational Change Management and Communication Plan.
2. Documentation of the Comprehensive Organizational Change Management and Communication Plan as described in this RFP.
3. Inclusion of organizational charts to integrate the Commonwealth and Vendor team.
4. Completion of the Business Process Mapping.
5. Creation of a map of the locations for the demonstrations and training.
6. Inclusion of enough detail to implement the change management and communication plan.
7. Completion of the Report of BPR Implementation – Success and/or opportunities for improvement.

Section 30.060.120.050—Deliverables

This section defines the Vendor Deliverables for the Organizational Change Management Activity. The table below identifies the Deliverable number and description; and the section where further information can be found in Appendix G – Deliverables.

Table 8 – Activity 6 Deliverables

NUMBER	DELIVERABLE	SECTION
6.1	Comprehensive Behavior Process Transition and Communication Plan	G.6.1
6.2	BPR Modeling of Future Processes	G.6.2
6.3	Training of Staff on New Processes	G.6.3
6.4	New Process Rollout	G.6.4
6.5	BPR Results Report	G.6.5

As a result of this activity, the Comprehensive Organizational Change Management and Communication Plan describes the Vendor's approach to integrating the Commonwealth and Vendor Project staffing teams and a plan to manage the expectations of varying groups of stakeholders who have different information needs. At a minimum, the plan should include:

1. The rebranding and marketing strategies for the MEMS and how to prepare end users for the changes to come.

2. The objectives, goals, and activities to be completed as well as the timeframe for completion.
3. Needs, expectations, and roles and responsibilities of stakeholders.
4. Identification and creation of leaders and power users throughout the end-user community and the roles these leaders should have with the business transition.
5. Communication change management methods and tools.

Section 30.060.130—Activity 7 – Acceptance Testing

The Vendor is responsible for facilitating Acceptance Testing of the entire MEMS to ensure that the new system meets the functional, technical, and operational requirements of CHFS. CHFS is responsible for participating in Acceptance Testing and for system sign-off and acceptance. CHFS sign-off on Acceptance Testing is a prerequisite to Activity 9, Implementation. Acceptance testing should focus on structured system testing, and operations readiness and load testing. Critical deficiencies identified during Acceptance Testing may require the Vendor to conduct rework defined in Activities 2 through 5 and modification of the associated deliverables before CHFS sign-off of the Acceptance Testing Activity and deliverables. Based on the Vendor's phased implementation plan, Acceptance Testing may be conducted in phases. Completion of this activity is the first step in CHFS's acceptance of the System.

Section 30.060.130.010—Objectives

1. The objective of the acceptance testing is to ensure that all requirements and related system functions are complete and accurate. Testing should assure the operations and hardware/software/telecommunications aspects of the new MEMS are functioning as designed. Testing should demonstrate that the new MEMS is ready to perform all functions including but not limited to processing inputs, paying and adjusting claims correctly, meeting reporting requirements, utilizing the State data communication network, and having a stable back-up and recovery capacity. Testing should include actual claims processing in a full operational environment from receipt of claims through financial processing, history update, and reporting.
2. The new MEMS should be tested under maximum operational load conditions and should include production of output files and reports. Claim volume testing and new MEMS interface transactions volume testing should also be conducted to demonstrate the systems production capacity. Production and test data should not be co-mingled.
3. All data interfaces to other applications and systems (incoming and outgoing) must be thoroughly tested in order to facilitate a successful transition to the MEMS system.
4. Operational Readiness testing should measure the competency, skill level, and proficiency of the FA Vendor staff and operations during workflow simulations and testing while demonstrating Medicaid business outcomes.
5. The Vendor should deliver a testing environment that simulates the production environment including workstations, telecommunications, a security layer, hardware and MEMS application software, and the use of representative test

data. The test environment should utilize separate data files from the production system. The Vendor should schedule and provide access to the test environment for CHFS staff and the Quality Assurance Vendor.

Section 30.060.130.020—Letter Certifying that the MEMS Is Ready for User Acceptance Testing (UAT)

The Vendor must issue a letter to CHFS certifying that: all data, user manuals, testing facilities, and security accesses necessary to perform UAT have been provided and CHFS must approve of the content of the letter. As stated in the Conversion Plan, the data used for UAT should be based on converted data. The CHFS approved letter is the authorization for the Vendor to proceed to the next testing phase.

Section 30.060.130.030—CHFS Acceptance Test Responsibilities

CHFS responsibilities for the Acceptance Test activity are:

1. Conduct Acceptance Testing of MEMS requirements. CHFS will designate a sign-off authority and provide SME staff for each part of the Acceptance Test checklist and will conduct acceptance testing activities.
2. Document and report testing abnormalities.

Section 30.060.130.040—Vendor Acceptance Test Responsibilities

Vendor responsibilities for the Acceptance Test activity are:

1. Establish the Test Environment including implementation of an automated testing and defect/issue tracking tool. Provide an interface with sufficient capacity to allow the State network to provide CHFS access to the Test Environment.
2. Execute testing according to the Test Plan.
3. Facilitate acceptance testing as defined in the Test Plan.
4. Provide training to CHFS staff on the tools and methodology to support this activity.
5. Monitor and record testing results.
6. Document problem conditions discovered in testing requiring corrective action and resolution.
7. Correct identified problems, document modifications, and conduct re-testing.
8. Update system, user, and operations documentation and other activity deliverables as needed.
9. Prepare and submit draft test results and other deliverables for review.
10. Conduct walk-through of test results deliverables.
11. Submit updated Source Code Library.
12. Submit the Business Continuity Plan for Systems Operations and Maintenance.
13. Support the IV&V process as defined in the RFP.
14. Prepare and submit final deliverables for approval.

Section 30.060.130.050—Milestones

The critical milestones that affect the schedule or impact progress during the Acceptance Testing activity are:

1. CHFS approval of test environment.
2. CHFS approval of test results, including corrective action taken.
3. CHFS approval of updated user, system and operations documents.
4. CHFS approval of Source Code Library for acceptance testing.
5. CHFS approval of the Business Continuity Plan for Systems Operations and Maintenance.
6. CHFS approval of DSD Version 2.
7. CHFS approval of Acceptance Test completion. Acceptance test approval should be complete before proceeding to Activity 9 – Implementation.

Section 30.060.130.060—Deliverables

This Section defines the Vendor Deliverables related to the Acceptance Testing Activity. The table below identifies the Deliverable number and description; and the section where further information can be found in Appendix G – Deliverables.

Table 9 – Activity 7 Deliverables

NUMBER	DELIVERABLE	SECTION
7.1	Test Environment*	G.7.1
7.2	Acceptance Test Plan*	G.7.2
7.3	Acceptance Test Results*	G.7.3
7.4	Operational Test Plan*	G.7.4
7.5	Operational Acceptance Test Results*	G.7.5
7.6	Source Code Library - Version 2: Acceptance Testing Environment*	G.7.6
7.7	Business Continuity Plan for Systems Operations and Maintenance	G.7.7
7.8	Detailed System Design Version 2	G.7.8

Deliverables noted with an asterisk (*) should be approved prior to commencement of the Acceptance Testing Activity.

CHFS review of the Services and Deliverables of this activity should ensure that:

1. The acceptance test results are sufficient verification that system capabilities fulfill the requirements identified in Appendix A – MEMS Functional Requirements and Appendix B – MEMS Technical Requirements.
2. Designated CHFS representatives review and accept assigned MEMS requirements.
3. All detected critical errors are adequately addressed and testing is re-accomplished to assure the system meets requirements.
4. The DSD is updated to Version 2 to reflect any system changes that occurred as result of acceptance testing.
5. CHFS approves the system for transition to the Implementation Activity based in an agreement that defines open system errors.
6. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.140—Activity 8 – Training (Section 60.010.010.070)

Training is a critical Vendor responsibility. The Vendor should provide training to all staff using the new MEMS including the Provider community. The strategy and plans prepared in this activity should demonstrate an understanding of CHFS training requirements, the Vendor's role in the training activity, and the training-related activities that are needed to support the Data Conversion (Activity 5), Acceptance Testing (Activity 7), and Implementation (Activity 9) activities of the Project. A discussion of the methods proposed to develop and deliver training necessary to ensure effective use and reliable operation of the new MEMS should be included.

The Vendor should evaluate the effectiveness of the training to support CHFS staff capabilities and should recommend and support improvements during the first year of FA and IT operations.

Section 30.060.140.010—Objectives

The objective of the Training activity is to ensure that both CHFS and Vendor staff and DMS Providers have the appropriate level of knowledge and skill to effectively interface with the MEMS and to perform and execute all operating, maintenance, and business functions related to job responsibilities.

The Vendor should develop Training Plans and training support materials, including handouts, instructions or training outlines, classes, presentations and initial login administration to meet the individual knowledge and skill needs for CHFS staff (including Vendors and community-based partners). Training and training support materials should be based on approved user and operations manuals as well as procedures manuals developed by the Vendor in previous activities. All documentation should be available for use during acceptance testing to verify accuracy, comprehensiveness, understandability, and usability.

MEMS training needs to be provided for three identified groups:

1. CHFS Trainers.
2. MEMS users across CHFS including Providers and MCOs.
3. Technical staff that support the MEMS.

CHFS should assist in the identification of specific individuals to be included in the types of training based on the training strategy defined in the Vendor Training Strategy. Training for each group should encompass the following:

1. CHFS Trainers Group Training – Prior to conducting User and Provider Training, the Vendor provides training to the CHFS Training Group. This training should enable the CHFS Training Group to participate in Enterprise-wide training as needed and eventually assume full responsibility for on-going training beginning the second full year of operations.
2. MEMS User Training – The MEMS User Training includes a basic MEMS overview that provides a system orientation and basic operation for all CHFS MEMS users including Providers and MCO's. User training should be required in Vendor-provided locations throughout the State.

3. Technical Staff Training – Technical training emphasizes the understanding and skills needed to perform assigned duties in support of the new MEMS. Technical training is provided to all designated CHFS systems staff. Technical training includes Third Party Software basic training (e.g., third party database basic programming curriculum).

Login administration includes developing a plan for initially distributing passwords to CHFS users in conjunction with the training process. The Vendor should support login administration until the end of the Implementation Activity.

The Vendor is encouraged to use a combination of classroom and distance learning techniques (including Computer Based Training (CBT) and self-paced/self-guided Web-Based training modules) to implement training for CHFS staff and providers. The training requirements include access to a training room provided by the Vendor with the necessary equipment to train State and Vendor staff on the operation of the system. The Vendor should also address methodologies and tools for evaluation of training effectiveness.

Section 30.060.140.020—CHFS Training Responsibilities

CHFS responsibilities for the new MEMS training activity are:

1. Provide access to the list of participating providers for provider training activities.
2. Identify and assign CHFS staff to training. Manage CHFS staff attendance and participation.
3. Participate in user training sessions.
4. Participate in technical training sessions.
5. Assume responsibility for login administration after the completion of the Implementation Activity.

Section 30.060.140.030—Vendor Training Responsibilities

The Vendor responsibilities for the new MEMS training activity are:

1. Prepare the Training Plan including training schedule (including dates, times, locations, participants).
2. Prepare and establish training environment and facility and remote training capabilities. Provide an interface (100 MB Ethernet interface) with the State network to provide CHFS access to the training environment.
3. Prepare Training Materials.
4. Complete MEMS Login Administration activities.
5. Ensure that CHFS standards for security and training (including the American Disabilities Act) standards are adhered to.
6. Conduct walk-through of deliverables as needed.
7. Conduct training.
8. Assess and track learning by students.
9. Prepare and submit the Training Report.
10. Support the IV&V process as defined in the RFP.

Section 30.060.140.040—Milestones

The critical milestones that affect the schedule or impact progress during the Training activity are:

1. CHFS approval of Training Strategy Deliverable.
2. CHFS approval of Training Plan Deliverable.
3. CHFS approval of Training Materials (for each type of training).
4. CHFS approval of the Training Environment.
5. CHFS approval of completion the Training Report.

Section 30.060.140.050—Deliverables

This section defines the Vendor deliverables related to the training activity. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 10 – Activity 8 Deliverables

NUMBER	DELIVERABLE	SECTION
8.1	Training Strategy*	G.8.1
8.2	Training Plan*	G.8.2
8.3	Training Environment*	G.8.3
8.4	Training Materials*	G.8.4
8.5	Training Report*	G.8.5

Deliverables noted with an asterisk (*) should be approved prior to commencement of the Acceptance Testing Activity.

CHFS review of the services and deliverables of this activity should ensure that:

1. Training facilities and remote training capabilities are established well in advance of training events and provide a production like environment.
2. Training and user login administration is accomplished as planned and that training attendee feedback on the quality of the training is rated as level 4 or greater on a five-level rating system.
3. Training includes coverage of MEMS interfaces and reports.
4. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.150—Activity 9 – Implementation

The Vendor should plan and prepare for all aspects of the MEMS to be at full functionality on the go-live date. Before the start of the Implementation activity, all requirements should have been met through successful testing and should satisfy the functional and technological requirements and conversion tasks specified in the RFP and as documented during the requirements analysis and systems design activities.

The Vendor should describe its overall approach to implementation, ensuring that the MEMS is ready to be implemented and that CHFS approvals have been obtained to

begin operations, system, user, and security documentation should be complete. System response time and user and automated interfaces should be clearly assessed and operational.

The Implementation Phase should end upon successful implementation of the MEMS and resolution of start-up issues. CHFS acceptance of this activity should complete the acceptance of the system.

Section 30.060.150.010—Objectives

The objectives of the Implementation Activity are to install the new MEMS and to conduct operational tests of the system in production. The Vendor completes implementation activities in such a way that there is limited disruption to client and provider services. All functions should work efficiently, in a timely manner, and as designed.

Section 30.060.150.020—CHFS Implementation Responsibilities

CHFS responsibilities for the Implementation Activity are:

1. Provide approval to implement the new MEMS.
2. Implement and support the updated business processes that support the new MEMS.

Section 30.060.150.030—Vendor Implementation Responsibilities

Vendor responsibilities for the Implementation Activity are:

1. Establish the production environment as defined in the Implementation Plan, including software installation, site preparation, and installation schedule.
2. Conduct final data and file conversion activities.
3. Conduct final system interface tests.
4. Update and produce final system documentation including Source Code Library – Version 3, User Manual – Version 2, Operating Procedures Version 2, Implementation Plan – Version 3 and other documentation as needed.
5. Conduct walk-through of deliverables. Obtain CHFS comments on draft deliverables.
6. Coordinate implementation efforts with the MCO's.
7. Implement and support the operation of the new MEMS, including providing Help Desk support (Level 1, 2, and 3) and connectivity issues.
8. Support the IV&V process as defined in the RFP.
9. Prepare and submit final deliverables for approval.
10. Obtain approval from CHFS to implement the system.
11. Implement the MEMS.
12. Ensure the optimal processing of the new MEMS, including production monitoring, emergency maintenance, and assistance in computer resource management and data resource management activities during the first 90 calendar days of operation.

13. Monitor system processing and performance to ensure that all functions and features are operating correctly, and correct any errors identified during the initial operations period.

Section 30.060.150.040—Milestones

The critical milestones that affect the schedule or impact progress during the Implementation activity are:

1. Documentation demonstrating that the production environment is established.
2. Documentation demonstrating that the final data and file conversion activities have been completed and tested.
3. Documentation demonstrating that the final system interface testing has been completed and documented.
4. Walk-through of final system, user, and operations documentation with CHFS staff.
5. Approval of final documents by CHFS staff.
6. CHFS approval of Final Implementation Plan deliverable.
7. CHFS approval of Source Code Library for Production Environment deliverable.
8. Delivery of the Implementation Certification Letter.
9. CHFS approval to proceed with Implementation.

Section 30.060.150.050—Deliverables

This Section defines the Vendor deliverables related to the new MEMS Implementation. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 11 – Activity 9 Deliverables

NUMBER	DELIVERABLE	SECTION
9.1	Implementation Plan – Version 3*	G.9.1
9.2	Production Environment*	G.9.2
9.3	Source Code Library – Version 3: Production Environment*	G.9.3
9.4	User Manual – Version 2	G.9.4
9.5	Operating Procedures – Version 2*	G.9.5
9.6	Final System Documentation DSD Version 3	G.9.6
9.7	Implementation Certification Letter	G.9.7

Deliverables noted with an asterisk (*) should be approved prior to commencement of the Acceptance Testing Activity.

CHFS review of the services and deliverables of this activity should ensure that:

1. For the implementation period, the Vendor demonstrates that the MEMS meets the performance standards identified in section 40.075.
2. All functions and features are operating to meet requirements and are available to all MEMS users.

3. The DSD Version 2 is updated to reflect any resolution of non critical defects and transition to Final System Documentation (DSD Version 3).
4. Based on proven operations, the system is accepted by CHFS.
5. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.160—Activity 10 – Operations – Fiscal Agent Services

This section describes the Vendor's FA responsibilities and performance expectations for business and program functions related to the core MEMS, its modules, and system components. The Vendor will provide on-going FA services for up to 5 base years and three, 1-year option periods to be exercised by DMS.

The Vendor should perform all business functions described in Appendix A – MEMS Functional Requirements and Appendix M – MEMS Fiscal Agent Responsibilities from the date of implementation of each component until each business function is turned over to a successor fiscal agent at the end of the Contract, including any optional additional periods or extensions. CHFS will monitor and review Fiscal Agent operations activities for enforcement of Contract provisions, accurate timely processing of fee for service claims, quality of call customer service, and other activities as described in the master SLA (Section 40. – Contract Terms and Conditions). The Vendor will be responsible for executing the Fiscal Agent operations of the MEMS on behalf of the State and will have the authority to pay claims and execute other financial management functions of the Kentucky Medicaid Program.

Section 30.060.160.010—Objectives

The objective of this activity is to ensure that the Vendor provides the proper level of operational support for all critical business areas to meet or exceed the Commonwealth's performance expectations and performance standards identified in the SOW. In conjunction with ensuring the proper level of support, the Vendor should show its commitment by providing staff resources that are skilled, experienced, competent and capable of delivering: Client Management Services, Provider Management Services, and Financial Management Services.

In addition, the Vendor should maintain consistent quality standards. The Vendor should deliver a Quality Management Plan to CHFS 90 days before the scheduled start of operations. The plan should address the Vendors commitment to retaining the personnel skills, and competency levels originally proposed for project operation as well as explain the philosophy and approach to the organizational operating quality culture that together should drive the efficient delivery of all MEMS services and meet performance expectations.

Section 30.060.160.020—CHFS Responsibilities

CHFS responsibilities for the Operations Activity are:

1. Provide contract and administrative oversight.
2. Negotiate all contract amendments and changes to the Contract.

3. Make policies, rules, and establish procedures for all DMS programs and communicate changes to the Vendor.
4. Oversee the correction of errors and discrepancies resulting in file update processes.
5. Define benefit packages for all State health care programs within the MEMS and provide support to assist the Vendor enroll/disenroll clients into a managed care program; and any other health management programs.
6. Determine which individuals are eligible to receive benefits in accordance with assigned eligibility coverage groups, eligibility spans, and special program codes.
7. Approve rules and schedule for automated processes to identify Medicaid clients eligible for Medicare and buy-in, and to properly enroll and pay premiums:
8. Provide monitoring and oversight to provider and recipient call centers operated by the Vendor.
9. Monitor the quality of all key performance metrics and SLAs Performance through the use of reporting systems, audits, reports, sampling, and onsite inspection at any time
10. Approve all provider issuances, billing instructions, handbooks, bulletins, and/or notices developed by the Vendor.
11. Define the content, distribution and schedule for all communications to providers and clients.
12. Define content, format, frequency, and media for all reports.
13. Provide to the Vendor the drug codes, procedure codes, diagnosis codes, and categories of services requiring service authorization.
14. Authorize the collection of third party resource information from outside sources and prepare and initiate agreements with insurance companies, governmental agencies, and other entities for performing data matches between their files and the MEMS client file.
15. Establish all policy regarding claims administration.
16. Establish and provide rules governing the adjudication of all claims and encounters.
17. Provide additional Medicaid Quality Control (MQC) and review procedures.
18. Release funds for deposits made to the Kentucky Medicaid Disbursement account for funding provider payments.
19. Use reports to account for payments and payment recoveries and to monitor banking activities.
20. Approve design, development, work plans, policies, and procedures for all data administration activities.

Section 30.060.160.030—Vendor Responsibilities

FA operations responsibilities can be found in Appendix M – MEMS Fiscal Agent Responsibilities. The support activities for the Vendor include, but are not limited to:

1. Contract Management and administration.
2. Coordinate and lead the implementation of a Quality Assurance Program to measure the overall quality of operations and delivery of services.
3. Process and adjudicate all claims in the HIPAA-compliant electronic transaction formats.

4. Support other HIPAA-compliant transactions such as the 834 Benefit Enrollment and 820 Payment Order/Remittance Advice files necessary for managed care operations.
5. Provide remittance advices.
6. Provide Help Desk (utilizing HBE Contact Center infrastructure) support services (Level 1, 2, and 3) for all modules and system components, and perform provider relations functions including provider enrollment.
7. Provide TPL verification and lead processing.
8. Provide Health Care Program Premium processing.
9. Provide banking services.
10. Provide Project Facilities (includes facilities which may or may not include representatives of all business partners, subcontractors and Commonwealth staff assigned to monitor the new MEMS replacement system.
11. Management and reporting of all SLAs.
12. Coordinate and perform training for State and Vendor staff as well as Medicaid Providers.

The Systems Operations and Maintenance (O&M) support activities for the Core Medicaid Enterprise System and Systems Integrator are discussed in Activity 12.

Section 30.060.160.040—Milestones

The critical milestones that affect the schedule or impact progress during the System Support activity are:

1. CHFS approval of the Quality Management Plan (annually, including prior to the start of this phase).
2. CHFS approval of the Staffing Requirements Capability Report (annually, including prior to the start of this phase).
3. CHFS approval of Annual Status Report for Operations.
4. Vendor submission of bi-weekly Project Status Reports for Operations.

Section 30.060.160.050—Deliverables

This section defines the Vendor deliverables related to Operations of the new MEMS Implementation. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 12 – Activity 10 Deliverables

NUMBER	DELIVERABLE	SECTION
10.1	Quality Management Plan*	G.10.1
10.2	FA Staffing Requirements Capability Report*	G.10.2
10.3	Bi-Weekly Project Status Report for Operations	G.10.3
10.4	Annual Status Reports for Operations	G.10.4

Deliverables noted with an asterisk (*) should be approved prior to commencement of the Acceptance Testing Activity.

Section 30.060.170—Activity 11 – Certification

The system certification planning process typically starts during the final stages of development. As the effort transitions to the testing phase there is an aggressive effort to gather documents, evidence and artifacts that validate and verify the MEMS is operating as designed.

In order to obtain maximum FFP, the new MEMS must meet CMS requirements from the first day of operations. Throughout the planned and organized progression of the project, deliverable activities and review criteria have served as the building blocks for successful system certification. This activity completes all activities and assembles documentation necessary to substantiate compliance with CMS requirements and obtain CMS certification.

The Vendor must warrant that the system is operating as designed and all defects as evidenced during implementation have been addressed and are fully remediated to the State's satisfaction before final payment is awarded.

Section 30.060.170.010—Objectives

The objective of this phase is to obtain Federal certification for the MEMS. CHFS must apply for and receive system certification from CMS, by demonstrating that the system meets all requirements and performance standards before receiving full Federal matching funds. The Vendor should be responsible for ensuring that the new MEMS meets the standards for MMIS certification, as specified by CMS, for the DDI of the system by the completion of Activity 9, Implementation + 6 months. It is expected that Certification should be completed in stages throughout the DDI and Implementation phases with final certification completed within six months of implementation.

Section 30.060.170.020—CHFS Certification Responsibilities

CHFS responsibilities for the Certification activity are:

1. Notify CMS that the new MEMS is ready for certification.
2. Approve the composition of the certification team.
3. Prepare and submit the Certification Readiness Statement to CMS and coordinate the CMS Certification Review.

Section 30.060.170.030—Vendor Certification Responsibilities

Vendor responsibilities for the Certification Activity are:

1. Ensure that the MEMS meets Federal certification requirements defined in the most current version of Part 11 of the State Medicaid Manual (SMM). The systems documentation finalized by the Vendor should be used to support the certification process.
2. Participate in certification planning and prepare review materials to demonstrate system compliance with certification criteria.

3. Prepare a CMS readiness checklist to assist DMS in the “go-live” decision, prior to “go live.”
4. Capture all appropriate artifacts to support the certification process.
5. Prepare presentation materials for DMS to review.
6. Provide copies of all system outputs needed to demonstrate full functionality back to the start of operations.
7. Participate, as necessary, during the Federal onsite certification review.
8. Assist CHFS in locating material needed to answer review team questions.
9. Provide any additional materials needed to resolve any post-review corrective actions.
10. Retain operations staff to provide post-implementation support during the initial months of operations through certification.
11. Support the IV&V process as defined in RFP.
12. Resolve any and all corrective actions needed to finalize Federal certification, with DMS approval.

Section 30.060.170.040—Milestones

The critical milestones that affect the schedule or impact progress during the Certification activity are:

1. Walk-through of draft deliverables.
2. CHFS approval of Certification Checklist deliverable.
3. CHFS approval of Certification Review Package deliverable.
4. CHFS notification to CMS that the system is ready for certification review and scheduling of certification review.
5. Successful certification.

Section 30.060.170.050—Deliverables

This section defines the Vendor Deliverables related to Certification. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 13 – Activity 11 Deliverables

NUMBER	DELIVERABLE	SECTION
11.1	Certification Checklist*	G.11.1
11.2	Certification Review Package*	G.11.2

Deliverables noted with an asterisk (*) should be approved prior to commencement of other systems development activities.

CHFS review of the services and deliverables of this activity should ensure that:

1. The MEMS becomes certified by CMS.
2. Deliverables meet the minimum requirements defined in Appendix G – Deliverables.

Section 30.060.180—Activity 12 – Software Maintenance and Modifications (Section 60.010.010.120)

This section describes the Vendor's software support responsibilities and performance expectations for the new MEMS.

The Vendor provides ongoing maintenance and modification support for the new MEMS for the same contract period, up to 5 base years and three, 1-year option periods. Ongoing changes, corrections, or enhancements to the system should be characterized as either maintenance-related or as a modification effort. The Commonwealth or the Vendor determines that a deficiency exists within the operational MEMS, including deficiencies (defects) found after implementation of modifications incorporated into the operational MEMS, which needs corrective maintenance.

Corrections (including development, testing, training and implementation) should be made for any of the following:

a. Deficiency or problem with the application functionality of the transfer system.
b. Deficiency or problem with the functionality developed or implemented.
c. Deficiency or problem with the functionality of subsequent system enhancements.

Modifications to the software should go through the formal change control process. CHFS is requiring 25,000 hours of Vendor-categorized staff time per contract year to apply towards system modification, changes, and enhancements to the MEMS once the system has been fully implemented for the life of the contract. The Vendor should analyze the change request, provide an estimate to CHFS, and receive approval prior to expending any of these hours. Defects will not be corrected utilizing any of these 25,000 hours. Any hours remaining at the end of a contract year will be rolled over to the next year.

System hosting, operations, and disaster recovery services are an "Option to Buy" which may or may not be exercised by the Commonwealth (See Section 30.060.260.010).

Section 30.060.180.010—Objectives

The objective of this activity is to ensure that the Vendor provides the proper level of software maintenance and modification support service, including meeting the performance standards identified in Section 40.075. This includes ensuring that an appropriate level of Vendor staff resources is identified to reliably operate, maintain and enhance the new MEMS modules and system components.

Section 30.060.180.020—CHFS Responsibilities

CHFS Responsibilities for this activity include:

1. Execute upgrades to CHFS network and desktops.
2. Provide information on changes in State policy and system requirements.
3. Approve the priority and order of changes related to business requirements or other changes to CHFS business processes identified by the Vendor or CHFS.
4. Evaluate and approve technical and design specifications for modifications.

5. Approve changes to technical and functional documentation.
6. Participate in testing process, including user acceptance testing of modifications.
7. Maintain administration of user access to applications.
8. Participate in the SOA Governance Committee meetings.

Section 30.060.180.030—Vendor Responsibilities

Vendor Responsibilities for this activity include the following services:

1. Preparation and submission of the Systems Support Plan (Deliverable 12.1), the Staffing Requirements Capability Report (Deliverable 12.2), and the Operations and Maintenance Procedure Manual (Deliverable 12.6).
2. Account/Project Management Services, including regular bi-weekly and annual status reports (Deliverables 12.2 and 12.3), and presentation of system status as requested by the MEMS Contracts Manager.
3. Software modifications, updates, changes, and enhancements to MEMS modules and system components for new and updated requirements and accordingly, the delivery of System Documentation Updates (Deliverable 12.5). The Vendor should use the configuration plan and software development methodology utilized in Activities 1-12, which includes support for updating MEMS training materials and other systems documentation.
4. Routine system maintenance to correct software errors and perform associated problem tracking and resolution.
5. General maintenance functions to maintain operation efficiency at the level, standards, and conditions the MEMS was originally approved.
6. Assistance with the identification, prioritization, and categorization of changes to business requirements as they relate to the functional areas and MECT business processes.
7. Development of the O&M Procedures Manual including audits and edits and other routine documentation.
8. Ongoing management of SOA integration services which should include:
   a. Operation and maintenance of the SOA framework and ESB.
   b. Developing standards, templates, policies, and procedures.
   c. With the assistance of the State, establishing the SOA Governance Committee and conducting meetings as specified by the State.
   d. Ensuring that all interfaces utilize established standards and advance CMS modularity and interoperability requirement initiatives.
   e. Management and administration of all Open and Application Programming Interfaces (APIs).
   f. Coordination and implementation of technical and operational requirements for the integration functions.
   g. Definition of the Enterprise Information Model and system interfaces.
   h. Assessing inventory and maintaining documentation of all interfaces via the Interface Control Document (ICD).
   i. Developing and maintaining the Service Registry.
   j. Implementing and managing the Information Technology Infrastructure Library (ITIL).

Section 30.060.180.040—Milestones

The critical milestones that affect the schedule or impact progress during the System Support activity are:

1. CHFS approval of the Systems Support Plan (annually, including prior to the start of this phase).
2. CHFS approval of the Staffing Requirements Capability Report (annually, including prior to the start of this phase).
3. CHFS approval of the O&M Procedures Manual (annually, including prior to the start of this phase).
4. CHFS approval of Annual Status Report.
5. Vendor submission of bi-weekly Project Status Reports.

These milestones should apply to modules and system components delivered and accepted by CHFS prior to the full implementation of the MEMS. At that time, these milestones should become applicable for the new MEMS as a whole.

Section 30.060.180.050—Deliverables

This section defines the Vendor deliverables related to Systems O&M Support of the MEMS. The Vendor meets the requirements for deliverables presented in Appendix G – Deliverables. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 14 – Activity 12 Deliverables

NUMBER	DELIVERABLE	SECTION
12.1	Systems Support Plan	G.12.1
12.2	Staffing Requirements Capability Report	G.12.2
12.3	Bi-Weekly Status Report	G.12.3
12.4	Annual Status Report	G.12.4
12.5	System Documentation Updates - Requirements Document - System Architecture and Design - Test Plan - Test Report - User Manual - Operating Procedures - Source Code Library - Training Materials - Workflow Processes	G.12.5
12.6	Operations and Maintenance Procedure Manual	G.12.6

Section 30.060.190—Activity 13 – Turnover

This Activity will be exercised by CHFS at the end of the Contract period. When CHFS exercises this Activity, the Vendor is required to transfer FA responsibilities and O&M support services for the MEMS to a successor Vendor (designee). The Vendor should cooperate with the successor Fiscal Agent, other Vendors, and CHFS in the planning and transfer of the MEMS and operations. The Vendor should dedicate special additional resources to this phase. This phase will begin 12 months before the end of

the Contract period and end 6 months after the end of the Contract period, or as extended by the exercise of Contract provisions or amendments to the Contract. This section describes the Activities necessary to ensure a smooth turnover of the MEMS and FA service responsibilities defined in Appendix A – MEMS Functional Requirements and Appendix M – MEMS Fiscal Agent Responsibilities.

At the beginning of the Turnover Phase, the Vendor should provide CHFS current operational and systematic processing procedures, data, and documentation or other information on a schedule as required by CHFS.

Section 30.060.190.010—Objectives

The Vendor provides full support and assistance in turning over the complete and current MEMS to a successor Vendor. CHFS desires a low-risk turnover that is transparent to recipients, providers, and users. Specific objectives are to provide for an orderly, complete, and controlled transition to the successor Vendor and to minimize any disruption of processing and services provided to clients, providers, and operational users of the MEMS.

Section 30.060.190.020—CHFS Responsibilities

This section identifies the responsibilities of the State with regard to initiating and facilitating transition activities in order to transfer or replace the existing MEMS.

1. Notify the Vendor of CHFS's intent to transfer or replace the system at least one (1) year prior to the end of the Contract by providing the Vendor with a “Letter of Intent to Turnover” the MEMS.
2. Review and approve a turnover plan to facilitate transfer of the MEMS to CHFS or to its designated agent.
3. Review and approve a statement of resources, which would be required to take over operation of the MEMS.
4. Make CHFS staff or designated agent staff available to be trained in the operation of the MEMS, if applicable.
5. Coordinate the transfer of MEMS documentation (in hard and soft copy formats), software and data files.
6. Review and approve a turnover results report that documents completion of each step of the turnover plan.
7. Review and accept data from conversion.

CHFS will exercise this activity by providing to the Vendor a “Letter of Intent to Exercise” Activity 13, 12 months before turnover (turnover begins after the last day of Activity 11 and 12) is to be completed. The Vendor should respond with a Proposal for Activity 13 within 15 calendar days. After reviewing and negotiating the Vendor’s proposal for Activity 13, CHFS will amend the Contract and extend the Contract Term for Post-turnover Services.

CHFS will oversee the MEMS turnover activity, ensuring that the incumbent Vendor adheres to the responsibilities and expectations set forth in the approved Turnover Plan

(Deliverable 13.1) and that resources identified in the Requirements Statement (Deliverable 13.2) are in place to enable transition activities.

Section 30.060.190.030—Vendor Responsibilities

Vendor responsibilities for Turnover include the following subtasks:

1. Prepare a Turnover Plan 20 business days following the start of Activity 13, the Vendor should provide to DMS a Turnover Plan. The Plan should include a Project Schedule/WBS as described in Appendix G – Deliverables for MEMS turnover activities and submit the schedule for CHFS approval.
2. Furnish to CHFS a Resource Requirements Statement, at no extra charge, a complete statement of all resources (personnel, hardware, software and facilities) needed and required by the State or another Vendor to take over operation of the MEMS, Correct Data Errors: The Vendor should be responsible for correcting data errors during the conversion process.
3. Agree to cooperate with the successor while providing all required turnover services. This should include meeting with the successor and devising work schedules that are agreeable for both CHFS and the successor.
4. On a schedule determined by CHFS, turn over all archived material including the Source Code Library electronically or on a medium approved by CHFS. The Vendor is required to transfer all active data, files, and tables electronically or on a medium approved by CHFS.
5. Appoint an appropriately skilled person (subject to CHFS approval) to manage and coordinate all turnover activities. The Vendor should not reduce operational staffing levels during the turnover period without prior written approval of CHFS.

The Vendor is also responsible for, and must correct at no cost, any malfunctions that existed in the system prior to turnover or which were caused by lack of support at turnover, as may be determined by CHFS, for up to 6 months following the turnover of operations.

Section 30.060.190.040—Milestones

The critical milestones that affect the schedule or impact progress during the Transition Activity are:

1. CHFS initiates Activity 13 with written notice.
2. Turnover Plan and Resource Requirements Statement are submitted and approved by CHFS.
3. Turnover Services are complete and turnover Results Report is submitted and approved by CHFS.
4. Post-turnover Services are completed.

Section 30.060.190.050—Deliverables

This section defines the Vendor Deliverables related to the Turnover Activities. The Vendor meets the requirements for Deliverables presented in Appendix G –

Deliverables. The table below identifies the Deliverable number and description, and the section where further information can be found in Appendix G – Deliverables.

Table 15 – Activity 13 Deliverables

NUMBER	DELIVERABLE	SECTION
13.1	Turnover Plan	G.13.1
13.2	Resource Requirements Statement	G.13.2
13.3	Systems Documentation	G.13.3
13.4	Source Code Library	G.13.4
13.5	Turnover Results Report	Vendor Format

Section 30.060.200—Reviews

In addition to the Deliverables listed in Appendix G, the selected Vendor is also responsible for creating any artifact or documentation that is required by a CMS review, or for approval of the MEMS solution, that is not covered in a listed Deliverable.

Section 30.060.200.010—CMS Gateway Reviews

At this time, CMS is not requiring the eight Gateway Reviews, prescribed in CMS's Exchange Life Cycle (ELC), referred to in the Collaborative Environment and Life Cycle Governance – Exchange Reference Architecture Supplement, Appendix S to this RFP, for MEMS development. During the DDI period, should CMS require the eight Gateway Reviews, the Vendor should be prepared to provide the following reviews listed below.

Reviews consist of an independent confirmation that project managers satisfactorily produced all the required deliverables and adequately met all exit criteria for the phase to permit advancement to the next phase. The selected Vendor's project manager is also responsible for providing documentation of known issues and plans to mitigate the risks, if any.

The Gateway reviews include:

1. R1 – Architecture Review (AR).
2. R2 – Project Startup Review (PSR).
3. R3 – Project Baseline Review (PBR).
4. R4 – Preliminary Design Review (PDR).
5. R5 – Detailed Design Review (DDR).
6. R6 – Final Detailed Design Review (FDDR).
7. R7 – Pre-Operational Readiness Review (PORR).
8. R8 – Operational Readiness Review (ORR).

Section 30.060.210—Functional Requirements

The functional requirements (Appendix A – MEMS Functional Requirements) apply to all Vendors participating in the project as well as those government and private entities, internal and external, who participate in the Kentucky Medicaid Enterprise Management System (MEMS) framework. The functional requirements have a strong impact on the relevance of the business and technical processes incorporated into the Kentucky enterprise-wide model through and beyond the systems project development phase. The functional requirements articulated in this Section of the document seek to achieve the following objectives:

1. Meet stakeholder needs.
2. Align the IT architecture with the business needs.
3. Seamless integration and data sharing.
4. Security and dependability.
5. Data integrity and consistency.
6. Reduce duplication.

The Functional Requirements cover the business operations of the enterprise. These requirements are grouped as follows:

1. Business Relationship Management.
2. Care Management.
3. Contractor Management.
4. Financial Management.
5. Member Management.
6. Operations Management.
7. Program Management.
8. Program Integrity Management.
9. Provider Management.
10. Additional business areas identified by the MECT Checklists.

Appendix A – MEMS Functional Requirements contains all the functional requirements. Each business area has a sheet with their specific requirements. The requirements are cross referenced to those identified in the MECT. It is conceivable that a requirement may show up on several spreadsheets if it impacts a number of different business areas.

Section 30.060.220—Fiscal Agent Responsibilities

This section describes the Vendor's FA responsibilities and performance expectations for business and program functions related to the core MEMS, its modules, and system components.

The FA plays a significant role in the Kentucky Medicaid Program. Responsibilities of the FA include:

1. Day-to-day activities

a. Contract administration.
b. Key personnel activities.
c. Mailroom.
d. Claims receipt, pre-screening, and conversion of claims/documents to micro-media.
e. Imaging/data entry (hard-copy and electronic transactions).
f. Receipt of data information from other DMS-specified interfaces.
g. Exception claims processing (non-medical suspense resolution).
h. Check request-related activities.
i. Finance-related business operations (accounts receivable handling, cash activity, etc.).
j. Report development and printing.

2. Operations of the MEMS, including, but not limited to:
   a. Acceptance, processing, and distribution of mail including imaging.
   b. Enrollment of FFS and MCO providers.
   c. Enrollment and credentialing of certain provider types, such as hospitals and nursing homes.
   d. Editing of all claims, adjustments, and mass adjustments.
   e. Correction of suspended claims.
   f. Distribution of Remittance Advices (RAs) and Explanations of Medicare Benefits (EOMBs).
   g. Determining and resolving TPL discrepancies and recoveries.
   h. FFS Prior Authorization (PA) processing.
   i. Imaging provider documentation, prior authorizations, checks, etc.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out. These responsibilities are aligned with the business areas specified in the Functional Requirements.

Section 30.060.220.010—Business Relationship Management

The Business Relationship Management business area encompasses those relationships that do not require contracts and may or may not require an exchange of data. Some of these relationships may be formalized by Memoranda of Understanding (MOUs), while others are more informal in nature. Electronic exchange of data is not always required, but there may be an exchange of information. These relationships are more critical as Electronic Health Records (EHRs) become more prevalent and covered entities develop policies regarding how related clinical data may be exchanged.

This area includes the following processes:

1. Establish Business Relationship.
2. Terminate Business Relationship.
3. Manage Business Relationship.
4. Manage Business Relationship Communication.

A primary need for the system is the ability to automate the tracking of business agreements. This would include notification of impending contract expiration so that new agreements (or termination) could be handled with a minimum of disruption.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Business Relationship Management functional requirements can be found in Appendix A – MEMS Functional Requirements, Business Relationship Tab.

Section 30.060.220.020—Care Management

The Care Management business area illustrates the growing importance of care management as the Medicaid program evolves. Care Management collects information about the needs of the individual member, plan of treatment, targeted outcomes, and the individual's health status. It also contains business processes that have a common purpose (i.e., identify clients with special needs, assess needs, develop treatment plan, monitor and manage the plan, and report outcomes). This business area includes processes that support individual care management and population management. Population management targets groups of individuals with similar characteristics and needs and promotes health education and awareness. This area should work closely with the Managed Care Organizations with respect to analysis of the member population and future programs.

This area includes the following processes:

1. Establish Case.
2. Manage Case.
3. Manage Registry.
4. Manage Medicaid Population Health.

Improved reporting (both scheduled and ad hoc) would assist various areas associated with member care, including Program Integrity and personnel responsible for the administration of the waiver programs. This capability would also aid in the analysis of specific member groups in order to help identify needs.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Care Management functional requirements can be found in Appendix A – MEMS Functional Requirements, Care Management tab.

Section 30.060.220.030—Contractor Management

The Contractor Management business area accommodates states that have managed care contracts or a variety of outsourced contracts. Some states may, for example, group Provider and Contractor in one business area. The Contractor Management business area has a common focus (i.e., manage outsourced contracts), owns and uses a specific set of data (i.e., information about the contractor or the contract), and uses business processes that have a common purpose (i.e., solicitation, procurement, award, monitoring, management, and closeout of a variety of contract types).

This area includes the following processes:

1. Produce Administrative or Health Services RFP.
2. Award Administrative or Health Services Contract.
3. Manage Administrative or Health Services Contract.
4. Close Out Administrative or Health Services Contract.
5. Perform Contractor Outreach.
6. Manage Contractor Information.
7. Manage Contractor Communication.
8. Inquire Contractor Information.
9. Manage Contractor Grievance and Appeal.

Specific needs that have been identified include the ability to allow authorized personnel to view contract details (including financial history) online. The system should be designed to interface with the new E&E system, in order to share data and activity performed by the Vendor. Activities of the Managed Care Organizations should be closely monitored for adherence to Commonwealth goals and regulations.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Operations Management functional requirements can be found in Appendix A – MEMS Functional Requirements, operations Management tab.

Section 30.060.220.040—Financial Management

The Financial Management business area is a collection of business processes to support the payment of providers, managed care organizations, other agencies, insurers, Medicare premiums, and supports the receipt of payments from other insurers, providers, and member premiums and financial participation. These processes share a common set of payment- and receivables-related data. The Financial Management business area is responsible for the financial data store.

These processes include the following:

1. Perform Accounting Functions.
2. Manage State Funds.
3. Manage F-MAP.
4. Manage FFP for MMIS.
5. Formulate Budget.
6. Manage Provider Recoupment.
7. Manage TPL Recovery.
8. Manage Estate Recovery.
9. Manage Cost Settlement.
10. Manage Member Premium Payment.

11. Manage Capitation Payment.
12. Manage 1099s.
13. Prepare Provider EFT/Check.
14. Prepare Home and Community Based Services Payment.
15. Prepare Premium EFT.
16. Prepare Health Insurance Premium Payment.
17. Prepare Medicare Premium Payment.
18. Inquire Payment Status.
19. Manage Payment Information.

This area expressed the need to greatly increase the number and quality of automated processes in such activities as the creation of standard reports, calculation and posting payments to various entities, and interface with Managed Care Organizations and insurance companies in order to share pertinent information.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Financial Management functional requirements can be found in Appendix A – MEMS Functional Requirements, Financial Management tab.

Section 30.060.220.050—Member Management

The Member Management business area is a collection of business processes involved in communications between the Medicaid agency and the prospective or enrolled members and actions that the agency takes on behalf of the member. These processes share a common set of member-related data. The goal for this business area is to improve healthcare outcomes and raise the level of consumer satisfaction. The presence of Managed Care Organizations for the vast majority of the members adds another layer to the areas of communication. The activities of the MCOs allow the Medicaid agency to focus more on the long term health of the members (as opposed to day-to-day claims processing and administration). Many of the business processes in this area should be performed by the HBE/E&E system. This business area is transformed with more patient self-directed decision-making. The processes included in this area include:

1. Inquire Member Eligibility.
2. Manage Member Information.
3. Perform Population and Member Outreach.
4. Manage Applicant and Member Communication.
5. Manage Member Grievance and Appeal.

The Commonwealth is implementing the HBE/E&E system specifically to manage member eligibility. The ability to seamless interface with this proposed system is critical. Requirements sessions have also identified the need for a web portal with accurate, up-to-date information (available with proper authorization) concerning member history and

activity. Information should be available real time as often as feasible. This information should be available by using an intuitive ad hoc reporting tool. Data gathered from the MCOs should be accurate and consistent with the internal files found at the Managed Care Organizations.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Member functional requirements can be found in Appendix A – MEMS Functional Requirements, Member Management tab.

Section 30.060.220.060—Operations Management

The Operations Management business area is the focal point of most State Medicaid Enterprises today. It includes operations that support the payment of providers, managed care organizations (MCOs), other agencies, insurers, and Medicare premiums and support the receipt of payments from other insurers, providers, and member premiums. The execution of these operations is addressed in the Financial Management business area.

This business area focuses on payments and receivables and “owns” all information associated with service payment and receivables. Common business processes include validating requests for payment and determining payable amount; responding to premium payment schedules and determining payable amount; and identifying and pursuing recoveries.

These processes include:

1. Prepare EOB.
2. Produce EOB.
3. Manage Drug Rebate.
4. Price Claim/Value Encounter.
5. Edit Claims-Encounter.
6. Audit Claim-Encounter.
7. Calculate Spend-Down Amount.
8. Apply Mass Adjustment.
9. Apply Attachment.
10. Authorize Treatment Plan.
11. Authorize Service.
12. Authorize Referral.
13. Prepare Remittance Advice Encounter Report.

The Operations Management area expressed the need for an accurate and accessible audit trail, ability to review prior authorization records online, and the online storage and management of plan of care information. Improved management and modification of claim edits and audits is desired, with less dependence on technical support for modifications.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Operations Management functional requirements can be found in Appendix A – MEMS Functional Requirements, Operations Management tab.

Section 30.060.220.070—Program Management

The Program Management business area houses the strategic planning, policy making, monitoring, and oversight activities of the agency. These activities depend heavily on access to timely and accurate data and the use of analytical tools. This business area uses a specific set of data (i.e., information about the benefit plans covered, services rendered, expenditures, performance outcomes, and goals and objectives) and contains business processes that have a common purpose (i.e., managing the Medicaid program to achieve the agency's goals and objectives such as by meeting budget objectives, improving customer satisfaction, and improving quality and health outcomes).

This business area includes a wide range of planning, analysis, and decision-making activities, including benefit plan design, rate setting, healthcare outcome targets, and cost-management decisions. It also contains budget analysis, accounting, quality assessment, performance analysis, outcome analysis, continuity of operations plan, and information management.

This area includes the following processes:

1. Manage FFP for Services.
2. Draw and Report FFP.
3. Monitor Performance and Business Activity.
4. Develop and Manage Performance Measures Reporting.
5. Manage Program Information.
6. Maintain Benefits-Reference Information.
7. Maintain State Plan.
8. Develop and Maintain Program Policy.
9. Develop Agency Goals and Objectives.
10. Manage Rate Setting.
11. Develop and Maintain Benefit Package.
12. Designate Approved Service Drug Formulary.

Required Workflow and Management systems, along with improved Case Tracking, should aid the processes associated with this area. Cost avoidance reporting (both detail and summary) is desired in order to facilitate Third Party Liability processing.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Program Management functional requirements can be found in Appendix A – MEMS Functional Requirements, Program Management tab.

Section 30.060.220.080—Program Integrity Management

The Program Integrity business area incorporates those business activities that focus on program compliance (i.e., auditing and tracking medical necessity and appropriateness of care and quality of care, fraud, waste, and abuse, erroneous payments, and administrative abuses).

Program Integrity collects information about an individual provider or member (i.e., demographics; information about the case itself such as case manager identification, dates, actions, and status; and information about parties associated with the case). The business processes in this business area have a common purpose (i.e., to identify case, gather information, verify information, develop case, report on findings, make referrals, and resolve case). As with the previous business areas, a single business process may cover several types of cases. The input, output, shared data, and the business rules may differ by type of case, but the business process activities remain the same.

Processes within this area include:

1. Identify Candidate Case.
2. Manage Case.

Improved reporting capabilities are a primary need to allow personnel to perform these processes. Reporting tool should be accurate and intuitive, with inquiries against data as up-to-date as possible. Standard reports should be generated and available on schedule, along with group profiles and statistics used in this activity.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Program Integrity Management functional requirements can be found in Appendix A – MEMS Functional Requirements, Program Integrity tab.

Section 30.060.220.090—Provider Management

The Provider Management business area is a collection of business processes that focus on recruiting potential providers, supporting the needs of the population, maintaining information on the provider, and communicating with the provider community. The goal of this business area is to maintain a robust provider network that meets the needs of both beneficiaries and provider communities and allows the Commonwealth Medicaid agency to monitor and reward provider performance and improve healthcare outcomes. The Commonwealth provides most of its Medicaid services through MCOs. In most cases, within this business area the MCO is considered a provider. These processes include:

1. Enroll Provider.
2. Disenroll Provider.
3. Inquire Provider Information.
4. Manage Provider Communication.
5. Perform Provider Outreach.
6. Manage Provider Information.
7. Manage Provider Grievance and Appeal.

The Provider business processes serve as the control point and central source of information on all providers and provider applicants. Files are maintained that provide comprehensive information on each provider, billing agency, trading partner, and provider group participating in the Commonwealth programs. A primary focus identified during requirement sessions is improving methods of validating credentials of potential and existing/returning providers (using automated tools). Improved means of reviewing a provider's history and status through online, up-to-date inquiry and reporting was also identified as a priority. A robust web portal including the ability to enter and update application data, inquire into provider entity relationships and locations (including the storage and management of multiple addresses), and investigate provider service activity is also required. An intuitive and powerful ad hoc reporting tool providing accurate and up-to-date information is a necessity.

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Specific Provider functional requirements can be found in Appendix A – MEMS Functional Requirements, Provider Management tab.

Section 30.060.220.100—Additional Business Area Requirements

Appendix M-MEMS Fiscal Agent Responsibilities contains all the responsibilities the FA is expected to carry out.

Appendix A – MEMS Functional Requirements includes functional requirements related to other MECT Checklists in addition to the areas listed above.

Section 30.060.230—System Compliance

The Vendor should comply with all of the following laws, regulations, and rules.

Section 30.060.230.010—Patient Protection and Affordable Care Act

On March 23 and 30, 2010, President Barack Obama signed into law the Patient Protection and Affordable Care Act, Public Law 111-148 and the Health Care and Education Reconciliation Act, Public Law 111-152. The two laws are collectively referred to as the Affordable Care Act (ACA). The ACA seeks to create new competitive

health insurance markets, including the establishment of Health Benefits Exchanges that should provide access to affordable health benefits for all residents in each State. Each Health Benefits Exchange (HBE) should meet Federal approval to operate a State Exchange by January 1, 2013 and be capable of providing open enrollment services by October 2013.

Under provisions of the ACA, the Commonwealth of Kentucky may expand access to health insurance coverage to newly eligible individuals. More specifically, the ACA extends Medicaid eligibility coverage to childless adults under age 65 with incomes up to 133 percent of FPL. The MEMS must comply with all ACA standards and should interface with the HBE.

Section 30.060.230.020—Compliance with Federal Regulations and Standards

The MEMS must comply with the national standards as prescribed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Balanced Budget Act of 1997 and any other Federal requirements and should be kept in compliance with new and modified requirements.

Section 30.060.230.030—CMS Enhanced Funding Requirements

CMS is encouraging states to broaden their vision in implementing a “big picture” approach to improving the operation of their Medicaid Programs. These changes should occur at the “enterprise” level and prioritize global population health and financial goals while improving the coordination and delivery of care to each Medicaid beneficiary, with an emphasis on those who have the greatest health needs and highest costs.

On April 2011, CMS issued the “Enhanced Funding Requirements: Seven Conditions and Standards” Medicaid Information Technology (IT) Supplement (MITS-11-01-v1.0). The requirements outlined in the CMS Seven Conditions and Standards should be met for future MMIS procurements in order for states to qualify for enhanced funding. Kentucky fully expects that the new MEMS will qualify for the full Federal enhanced funding match.

The goal is to promote a cost-effective, competitive environment for reusable MMIS products that can sustain the growing demand for flexible, open, SOA systems in the MMIS marketplace environment. CHFS intends to procure a solution that meets the enhanced funding requirements.

Section 30.060.230.030.010—Compliance with CMS Seven Conditions and Standards (Section 60.020; 4.1)

In addition to meeting the above objectives, the new MEMS shall meet the conditions and standards for enhanced Federal match through the design, development, integration, implementation, and operation of a system that should:

Section 30.060.230.030.010.010—Be Modular

The new MEMS adheres to the CMS definition of a modular, flexible approach to systems development, including the use of open interfaces and exposed APIs; the separation of business rules from core programming; and the availability of business rules in both human and machine-readable formats. The commitment to formal system development methodology and open, reusable system architecture is extremely important in order to ensure that CHFS can more easily change and maintain systems, as well as integrate and interoperate with a clinical and administrative ecosystem designed to deliver customer-centric services and benefits.

The definition of Modularity is breaking down systems requirements into the lowest component parts and still be functional.

It is expected that the new system should be developed as part of an SOA. Modularity also helps address the challenges of customization. Baseline web services and capabilities can be developed for and used by anyone, with exceptions for specific business processes handled by a separate module that interoperates with the baseline modules. With modularity, changes can be made independently to the baseline capabilities without affecting how the extension works. By doing so, the design ensures that future iterations of software can be deployed without breaking custom functionality.

A. Use Systems Development Life Cycle Methodologies

CHFS wishes to allow each potential Vendor to bring to this development effort its industry-best-practice system development methodologies and tailor them to the DMS's needs. To encourage this and to foster the adoption of an integrated development approach, CHFS plans to rely on the evaluation of proposal methodologies to see how the deliverables and practices of these methodologies meet industry standard system and software engineering principles. It hopes that by adopting this approach, it should encourage innovation and agility while preserving its desired development outcomes. At a minimum, CHFS is expecting the Vendor's life cycle development approach to use the CMS Guidance for Exchange and Medicaid Information Technology (IT) Systems v 2.0 and higher. Within the life cycle, CHFS will encourage Vendors to identify items of risk and introduce them as early as possible. The "risk forward" approach may involve development or prototyping of high-risk items as soon as the project starts.

CHFS's goal is to benefit from an iterative or agile-based development approach focused on the delivery of working components generally, while retaining the ability to address high-risk items with a greater level of process discipline when needed. This approach is preferred due to the perceived need to respond and support rapid business changes that are forthcoming. CHFS will require from the Vendor a system development life cycle which can accommodate all these needs while balancing agility and traditional process discipline.

B. Emphasize Open Interfaces

The flexibility of open interfaces and exposed APIs as components for the service layer as set forth in the standards and conditions is a mandatory system

component. Kentucky has already identified all current and potential future interfaces see Appendix E.

C. Utilize a Rules Engine

The MEMS uses a business rules engine and separate business rules from core programming. CHFS has invested in the Corticon rules engine software for the HBE project and would prefer to leverage this in the MEMS; however, CHFS will consider other alternatives depending on the applicability of the solution.

CHFS requires business rules in both human- and machine-readable formats in order to submit to the HHS-designated repository in human-readable form so as to be made available to other states and to the public.

Section 30.060.230.030.010.020—Align and Advance in MITA Maturity (Section 60.020; Chapter 4.2)

MITA is an initiative of CMS, aligned with the National Health Infrastructure Initiative (NHII), and intended to foster integrated business and IT transformation across the Medicaid domain to improve the administration of the Medicaid program. The MITA objectives are specifically to:

1. Adopt data and industry standards.
2. Promote secure data exchange.
3. Promote reusable components through standard interfaces and modularity.
4. Promote efficient and effective data sharing to meet stakeholder needs.
5. Provide a customer-centric focus.
6. Support interoperability and integration using open architecture and data standards.
7. Support integration of clinical and administrative data to enable better decision-making.
8. Break down artificial boundaries between systems, geography, and funding (within the Medicaid program).

The overall MITA initiative reaches well beyond the scope of the MEMS, but the system plays a critical role in CHFS's ability to successfully implement and achieve the goals of MITA. MITA aims to incorporate many relevant standards into an architecture model that should be used to build and enhance Medicaid health care systems as well as the data exchange between system components and drive system design from a business and customer-centric perspective across the Medicaid enterprise.

MITA is a planning tool intended to support proactive, modular approaches to planning improvements to both the program and the supporting systems. The Agency intends to use this tool in the design and development of the new MEMS.

A. MITA SS-A and Roadmap

DMS completed a MITA 2.01 SS-A update in July 2012 and has plans to update its self-assessment as soon as possible upon the release of Version 3. Appendix Y identifies the To Be goals identified during the Assessment. These goals form

the basis of the Roadmap projects. These projects should enhance the Commonwealth's ability to improve efficiency and services for its stakeholders consistent with MITA principles. It is anticipated that with the implementation of the new MEMS that DMS should meet MML 2 requirements with several business areas achieving MML 3. This roadmap should be reviewed and updated annually, at a minimum, to review progress, as well as to update changes that should inevitably occur. DMS plans to continue the reengineering of business processes along the MITA continuum.

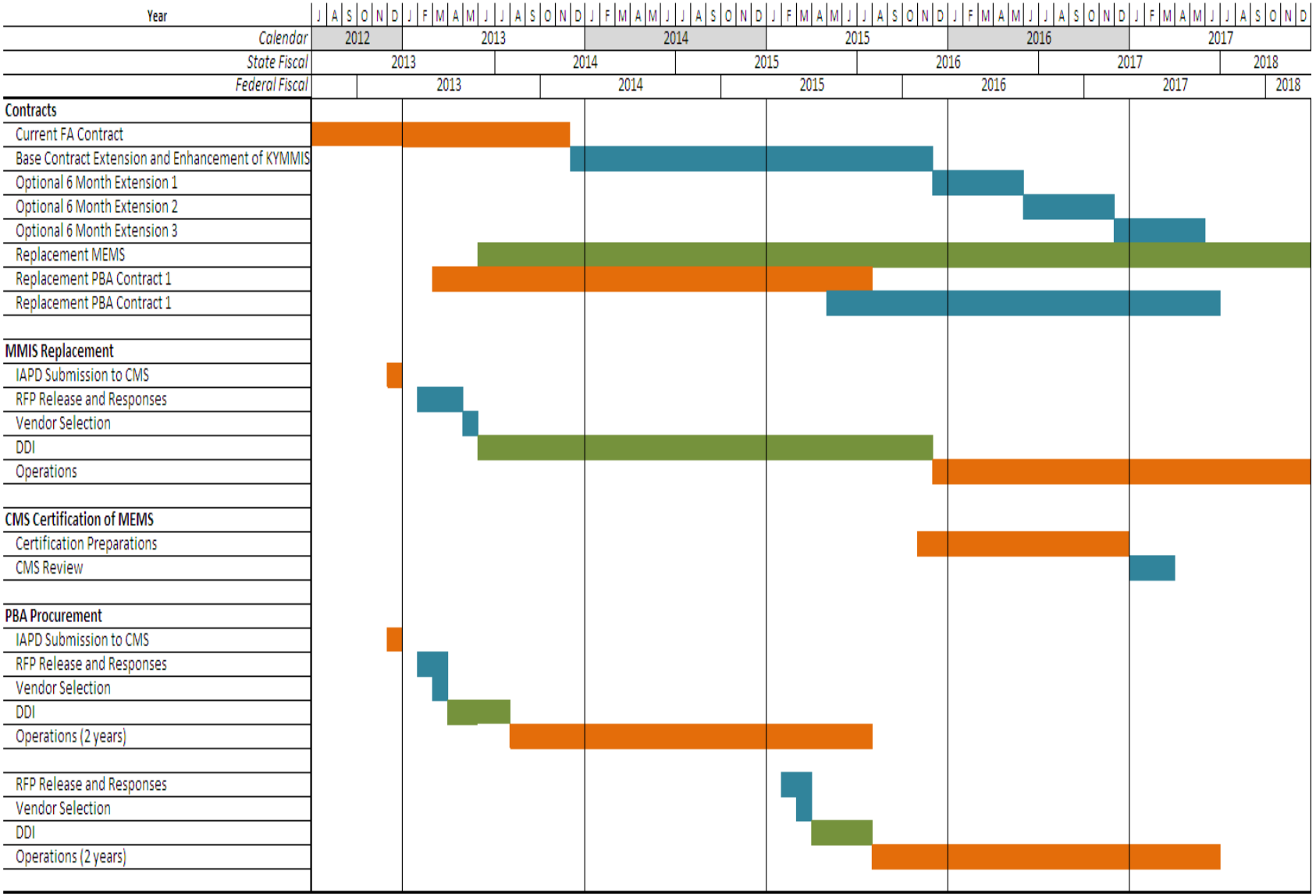

Figure 1 MITA Roadmap

The State is seeking an innovative MEMS solution that:

1. Supports the goals of the MITA framework.
2. Uses software engineering and system development life cycle methodologies as the basis to design new systems.
3. Uses proven methodologies and tools to develop new business processes and create information requirements for the new MEMS.
4. Uses proven operational management tools and processes to provide best-of-breed program and business services.

B. Concept of Operations (COO) and Business Process Models (BPMs)

The Vendor should be required to develop business process models for the purpose of continually streamlining and standardizing the business processes surrounding the MEMS. DMS will be continuing to work on aligning these business work flows as additional guidance is received from CMS.

As indicated previously, the MITA SS-A has ranked the processes surrounding the MEMS system at a MML 1.

Section 30.060.230.030.010.030—Meet Industry Standards

A. Identification of Industry Standards

CHFS wants assurance that the new MEMS aligns with, and incorporates industry standards including:

1. The HIPAA security, privacy, and transaction standards
    a. MITA supports facilitating automation where possible, and promotes using standards when developing and building automated processes. This is most apparent as MITA work efforts continue to move forward with developing standard data elements, file layouts, and other processes for efficient and effective data exchange to occur. Although such standards are not yet fully developed through the MITA initiative, the Vendor should use existing standards such as HIPAA-compliant eligibility transactions and be prepared to utilize new standards once available.
    b. Accessibility standards established under Section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities and compliance with Federal civil rights laws including production of a Section 508 Product Assessment Package as part of its System Development Life Cycle (SDLC). All products and services provided or developed as part of fulfilling this contract conforms to Section 508 of the Rehabilitation Act of 1973 and any amendments thereto, (29 U.S.C. & 794d), and its implementing Electronic and Information Technology Accessibility Standards (36 CFR § 1194). Section 508 requires that electronic and information technology is accessible to people with disabilities, including employees and members of the public. Information regarding accessibility under Section 508 is available at

http://www.section508.gov/, and a technical assistance document can be found at http://www.access-board.gov/sec508/guide/. Compliance testing is required.

c. Websites, web services, and web applications should be accessible to and usable by individuals with disabilities. This means any websites, web services, and/or web applications developed in the fulfillment of this contract — including, but not limited to any web-based training material, user documentation, reference material, or other communications materials intended for public or internal use related to the work completed under this contract.

2. Standards adopted by the Secretary under section 1104 of the ACA.
3. Standards and protocols adopted by the Secretary under Section 1561 of the ACA.
4. The National Information Exchange Model (NIEM) and unified form to develop, disseminate, and support standards and processes that enable the consistent, efficient, and transparent exchange of data elements between programs and states.
5. National Institute of Standards and Technology (NIST) security guidance and other standards as appropriate.
6. Section 6103 of the Internal Revenue Code.
7. Additional standards identified by CMS.
8. Industry standards promote reuse, data exchange, and reduction of administrative burden on patients, providers, and applicants.

B. Incorporation of industry standards in requirements, development, and testing phases

The Vendor should implement practices and procedures for the system development phases such as requirements analysis, system testing, and user acceptance testing (UAT). Plans should ensure that all systems comply fully and on-time with all industry standards adopted by the Secretary of HHS.

Section 30.060.230.030.010.040—Leverage Other State Systems

A. Reuse of efforts

Wherever possible, the new MEMS leverages and reuses technologies and systems from within the Commonwealth of Kentucky and other states. CHFS acknowledges that it can benefit substantially from the experience and investments of other states through the reuse of components and technologies already developed, consistent with an SOA, from publicly available or commercially sold components and products, and from the future use of cloud technologies to share infrastructure and applications. It is the Commonwealth's goal to find a solution that provides for shared releases of future functionality in an effort to provide reusability and cost containment.

B. Identification of open source, cloud-based and commercial products

Vendors are encouraged to provide solutions incorporating commercially or publicly available off-the-shelf or open source solutions, and discuss

considerations and plans for cloud computing. Vendors identify any ground-up development activity within their solution and why this approach has been proposed.

C. Customization

CHFS prefers a solution requiring as little customization as possible while still meeting all the requirements identified. Once a solution is identified it is expected that the Vendor should perform a gap analysis and identify gaps between the requirements and the solution.

D. Transition and retirement plans

CHFS is already in the process of identifying duplicative systems through collaboration with other Commonwealth Cabinets. One of the goals of this collaborative effort is to build upon existing public and private sector resources and capabilities to the greatest extent possible.

Section 30.060.230.030.010.050—Improve Business Results

A. Degree of Automation

Kentucky seeks the highest degree of automation possible and has documented this need throughout the requirements. Not only is automation for MEMS documented, but also for workflow, notice generation, redeterminations, and worker alerts. It is only through this high degree of automation that one can achieve efficiencies and accuracy.

B. Customer Service

DMS has continuously sought to improve customer service through the establishment of customer service centers, web applications, and a call center. CHFS will be furthering its efforts with the new system that will allow customers to access information regarding their accounts through a web portal.

C. Performance Standards

The Vendor should conform to performance standards, where applicable, in regards to the eligibility transactions and communications with applicants and members. DMS has identified several different performance standards for program improvement and these should undergo testing. If unable to meet system performance standards established, the Vendor should create and execute a Plan of Action to execute and correct. DMS expects the Vendor, if applicable, to identify what criteria or performance standards that its solution currently meets or exceeds.

Section 30.060.230.030.010.060 – Incorporate Reporting Conditions

CHFS has identified robust reporting requirements to produce transaction data, reports, and performance information through the use of dashboards, and ad hoc reporting. Appendix J – Report inventory includes the current list of reporting requirements.

Section 30.060.230.030.010.070—Be Interoperable

The MEMS should be built with the appropriate architecture and using standardized messaging and communication protocols in order to preserve the ability to efficiently, effectively, and appropriately exchange data with other programs. The Vendor assumes responsibility for knowing and understanding CHFS's environment (data, applications, and infrastructure) in order to map its data to information-sharing requirements. The data-sharing architecture should address the conceptual and logical mechanisms used for data sharing and should also address data semantics, data harmonization strategies, shared-data ownership, security and privacy implications of shared data, and the quality of shared data.

Section 30.060.230.040—Compliance with Commonwealth Regulations and Standards (Section 60.010.010.110)

All proposed solutions submitted in response to this RFP should be fully compatible with the CHFS's technical environment. In addition, the MEMS should meet the requirements identified in the SMM.

Section 30.060.230.050—CMS Certification

CHFS intends to meet all CMS MECT requirements. The requirements found in the MECT checklists have been incorporated into the RFP requirements. The MEMS must meet all Federal requirements for certification as prescribed in the SMM, Part 11, and will be certified. The CMS Certification requirements and activities are described in Attachment B – Scope of Work, Activity 11 – Certification.

Section 30.060.240—General System Requirements (Section 60.010.010.090)

CHFS is issuing this RFP to procure and implement a new MITA-compliant MEMS founded on SOA components. The MEMS should support the core operations of the Medicaid program and the Commonwealth Enterprise. It should be instrumental in supporting Kentucky's Health Care Reform initiatives. The MEMS should be closely linked to and aligned with the Commonwealth's Health Information Technology Plan, the Commonwealth's Blueprint for Health, and the Federal governmental initiatives under the ARRA, including the HITECH Act, and ACA. The MEMS is architected to support the Managed Care model.

The MEMS is integral to the Commonwealth's vision for the Enterprise Architecture with SOA components. The proposed MEMS should achieve the long-term goals and the vision for the next generation of Medicaid systems and the next version of MITA.

Section 30.060.240.010—System Documentation

The MEMS System Documentation should be prepared by the successful Vendor and provided to the State prior to final acceptance of the MEMS. MEMS System

Documentation should be provided to the State in hardcopy (as requested) as well as electronic form. MEMS System Documentation should be updated by the successful Vendor to reflect system changes. Updated documentation should be provided to the State prior to final acceptance of the system change.

Section 30.060.240.020—Technical Requirements (Section 60.010.010.050)

The Vendor adheres to the enterprise-wide technical requirements (Appendix B – MEMS Technical Requirements) without exception. The purpose is to establish a shared understanding of CHFS's vision as it relates to business processes and workflows, user interfaces, application/software architecture, and infrastructure/information architecture throughout the project life cycle. The interrelationships among these architectures and their joint properties are essential to the Kentucky enterprise-wide model and are intended to address the important enterprise-wide objectives of this project.

This section of the RFP outlines the narrative descriptions of each of the technical areas identified in Appendix B – Technical Requirements and should form the foundational platform upon which the Commonwealth's operational vision for the MEMS should be built.

Section 30.060.240.020.010—Access and Presentation Services

The Access and Presentation Services layer of the technical solution is the architecture layer that addresses all user interface components and system access channels. The system can be decomposed into two user interaction layers, access channels and presentation.

Section 30.060.240.020.020—Access and Presentation Services - Access Layer (ACC)

The system's access layer provides a flexible framework for managing and providing internal and external communications over a variety of different channels. Customers also have the flexibility to access services provided by the MEMS over a variety of channels that may include, but are not limited to, web, phone, email, or mail.

Section 30.060.240.020.030—Access and Presentation Services - Presentation Layer (PRE)

The presentation layer provides users access to the system using a robust, thin-client, browser based solution delivered over the Internet. The selected Vendor is required to adhere to CHFS graphical user interface (GUI) standards and policies. The site should provide services to persons with disabilities by complying with mandates listed in the Rehabilitation Act of 1973, Section 508 and W3C's Web Content Accessibility Guidelines 2.0. The public facing site should be accessible to individuals in English and Spanish, and should provide the ability to extend support to different languages in the

future. The solution should support usable, mobile-friendly browsing and enable access to the site's features and services using smart phones, tablets, and personal digital assistants (PDAs). The solution should also be extensible to support creation of and consumption by mobile applications (apps) in the future.

Section 30.060.240.020.040—Integration Services (INT)

The Integration Services layer of the MEMS technical solution is the architecture layer that enables sharing of application services. The layer enables the system to share data, information, and processes that operate across application boundaries.

The integration layer features a shared services offering provided by the Commonwealth for Enterprise Service Bus (ESB) capabilities. CHFS has chosen Microsoft BizTalk Server as the standard messaging infrastructure to be used for messaging, routing, guaranteed delivery, transformation, and translation. The ESB provides services for, but not limited to, SOAP XML web services, HL7, HIPAA, and legacy integrations.

Section 30.060.240.020.050—Application and Shared Services (APP)

The Application Services layer of the technical architecture is the layer that provides reusable commodity features and functions within the system. The Shared Services layer is a sub-set of Application Services that can be exposed externally to other systems, applications, or external entities for reuse.

The architecture features a set of services that are classified as Shared Services to promote reuse and leverage based on guidance from CMS.

The proposed system should feature a full-featured architecture component for developing, managing, maintaining, and versioning business rules external to application code. The business rules engine should provide the ability to: quickly adapt program rules to policy changes, maintain business rules using business analysts rather than developers, and express rules using language that can be understood by the general public. The solution should provide open standard interfaces so that it can be leveraged as a shared service.

The system should feature Application Services that should be utilized by the application to deliver basic commodity features and provide domain business services to the application. The system should include services for data integration with HBE/KAMES eligibility system, other state agencies, and the Federal Data Services Hub for eligibility information verification. CHFS mandates that application business services that are custom developed and require ongoing maintenance by CHFS be developed and delivered using the Microsoft technology stack, specifically the .NET platform.

Section 30.060.240.020.060—Data and Information Management Services (DAT)

The Data and Information Management Services layer of the technical solution is the architecture layer that provides services for data management. This layer includes the definition of data services, reporting and analytics components, and the master data management features of the system.

The data services layer should provide the application with highly-available, redundant, consistent data. The layer consists of the infrastructure, processes, and management tools required to deliver data services to the application.

Section 30.060.240.020.070—Infrastructure Services (INF)

The Infrastructure Services layer is the layer that provides the application servers, database platforms, programming libraries and runtime framework for the application. The Infrastructure Services layer should be designed to enable quality, high-performing, scalable delivery of application services to the end-user.

The Infrastructure Services layer should provide logical environments for each testing phase. The selected Vendor's infrastructure strategy should provide the ability to create, deploy, load and manage multiple environments that operate concurrently. The selected Vendor's environment strategy should closely align with the work stream and testing strategy.

The system should demonstrate fault tolerance and redundancy to prevent applications from becoming unavailable due to component failures. The system design should provide clustered application server environments, load balanced applications and application components, redundant application data and storage designs for all data stores (data, logs, messages, message queues, etc.).

Section 30.060.240.020.080—Security:
The Vendor should adhere to the Commonwealth Office of Technology (COT) security and enterprise policies and procedures and the CHFS security policies and procedures.

1. COT Enterprise policies can be viewed at http://technology.ky.gov/governance/Pages/policies.aspx
2. COT Security Procedures can be viewed at https://gotsource.ky.gov/docushare/dsweb/Get/Document-329691
3. CHFS Security Policies are available at http://chfs.ky.gov/os/oats/policies.htm

Section 30.060.240.020.080.010—Security Services

1. NIST baseline should be moderate.

2. Provide annually a SSAE 16 (or comparable review) to the CHFS for the Frankfort office location of the selected Vendor. The data center where the system is hosted must also provide an annual SSAE 16.
3. The Vendor must perform a Risk Assessment following HIPAA guidelines every 365 days.
4. Security Testing is required by the selected Vendor on functional, technical, and infrastructure components to ensure the system meets all system security requirements. Security Testing scenarios and strategy should be approved by the CHFS Information Security Office (CHFS ISO) prior to execution and all Security Testing results shall be approved by CHFS and CHFS ISO. Additionally, the selected Vendor is required to conduct its own security risk assessment prior to the Commonwealth engaging a Third Party Vendor to conduct the Independent Security Assessment. The selected Vendor shall provide a report of the results of its security risk assessment, including all tools used, such as code scanning and application scanning tools, and an action plan of remediation for vulnerabilities identified. The Vendor should have a third party security assessment done annually as required by CHFS/COT Policies.
5. The Vendor shall establish and maintain appropriate levels of disaster recovery and regularly test the established disaster recovery. The Vendor should discuss options available as part of the solution related to disaster recovery. It is the preference of CHFS that this include local hot swap/hot fail over redundancy in all critical components as well as hot site operations with database replication.

Section 30.060.240.020.080.020—Security Plan

The Security and the Privacy Impact Assessment should be included as a separate document of a part of the Detailed Design Document (DDD).

1. Provide a detailed in-depth data flow diagram of the KYMMIS system illustrating the security mechanisms.
2. Provide a detailed in-depth architectural diagram for the KYMMIS system to include all infrastructures.

Section 30.060.240.020.090 – HIPAA Compliance

The MEMS should be compliant with HIPAA rules for access, authentications, storage and auditing, and transmittal of electronic personal health information (e-PHI). Standards include HIPAA Version 5010 standards for electronic health transactions (effective January 1, 2012).

The MEMS HIPAA compliance controls and procedures should be submitted to CHFS for review and approval, prior to the inclusion of any of these controls in the overall System Design.

The selected Vendor is not permitted to use or disclose health information for any reason other than that mandated within this RFP.

Section 30.060.240.020.100—Operations and System Management Services (OPR)

The Operations and System Management Services layer is the architecture layer that provides system and application administration and monitoring capabilities.

The selected Vendor's solution should monitor and report the health and status of all applications, services, and system components for the solution. The application monitoring solution should provide operations users the ability to view health and availability of application resources, application uptime, and service utilization. The server resources should be monitored against similar server specific metrics. Adherence to MITA requires the collection of operational data in order to establish and meet Service Level Agreements (SLAs) for the system.

Section 30.060.240.020.110—Development Architecture and Services (DEV)

The selected Vendor should utilize a well established formal methodology that supports the Commonwealth's requirement to sign off on results of the solution before proceeding to the next development phase.

The selected Vendor's testing methodology should include full testing to include the following test cycles: unit testing, integration testing, performance testing, load testing, stress and capacity testing, data conversion testing, user acceptance testing, and disaster recovery testing.

Section 30.060.240.030—Architecture Requirements

CHFS has developed a technological roadmap for the Kentucky Quality Health Information (QHI) framework. The QHI facilitates the implementation of technology standards and approaches for the development of an interoperable, scalable and easily adaptable cross-sector technology framework.

Most of the legacy systems implemented in the past were on independent platforms creating individual monolithic architectures. Communication between systems is difficult as is aggregation and correlation of data in the enterprise. Kentucky is embracing the Medicaid Enterprise Solution (MES) architecture and should transition the existing system to align with this new system architecture. This new approach should promote interoperability, reusability and sharing information throughout the enterprise as well as across organizational boundaries.

Kentucky views the QHI as a house built on a solid foundation of a sharable technical services and a common enterprise service bus with various applications as pillars. The Commonwealth utilizes .Net as their technology platform. MEMS should align with this architecture wherever possible. (See the figure below.)

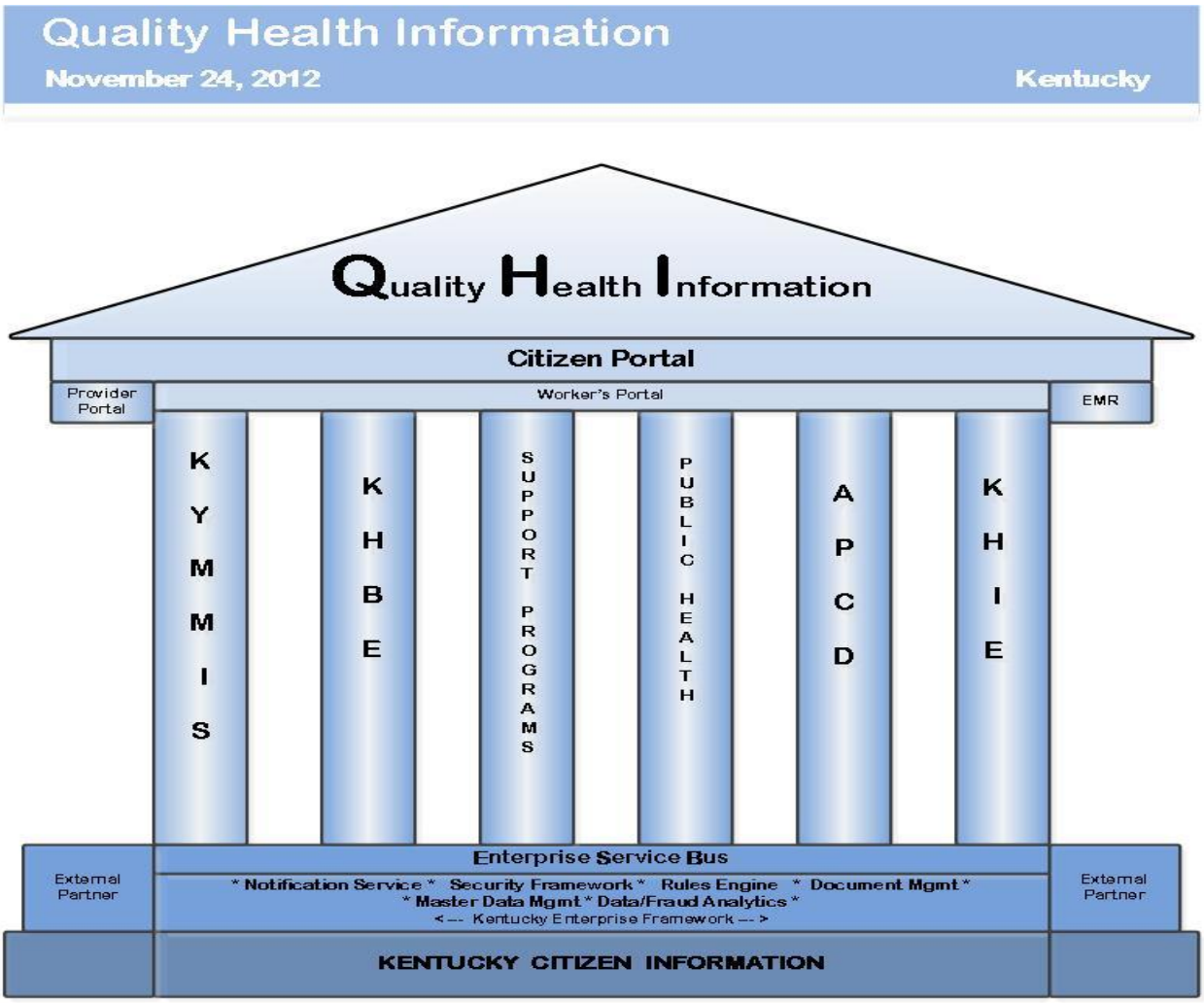

Figure 2 Quality Health Information

Components of the QHI:

1. **Portals:** The components of QHI should be accessed via Web Portals and Web interfaces by the users. The users are grouped into one of several broad categories such as: 1) Citizen, 2) Worker, and 3) Partners. Kentucky is embracing Microsoft technologies to build its web interfaces using Microsoft's web presentation patterns.

a. **Citizen Portal**: The purpose of the Citizen Portal is to provide access via single sign-on to view information including eligibility, status, and claims for benefits received from the Cabinet for Health and Family Services. In addition, it should also be a vehicle to view personal health record through the Kentucky Health Information Exchange (KHIE).

b. **EMR Interfaces**: Kentucky's vision is to build a foundation for connectivity for all EMRs to facilitate the exchange of health information between exchange participants. The QHI foundation should provide this connectivity to exchange information with the KHIE using web services or the ESB. The QHI foundation should enable EMR Vendors to incorporate into physicians practice workflow access to all applicable KY State applications and reporting services. For example, a physician could retrieve a report directly from the State's Prescription Monitoring Program system through EMR interface without leaving his/her EMR.

2. **Common Technical Services:** Kentucky's approach to QHI construction is first to build its foundation with a sharable technical services platform. Initially, the following technical services should be made available for the enterprise applications.

   a. **Document Management Services (DMS):** KY has opted to use Microsoft SharePoint 2010 server platform to build its DMS. It has chosen this platform for its new features. DMS will provide components to process and store all electronic documents. In addition, it will also index the documents for faster retrieval. KY expects the volume to be in the range of 300-500 million in the next five years. MEMS should utilize this system where appropriate.

   b. **Business Rules Engine (BRE):** KY has opted to implement Corticon's Business Rule Engine (BRE) to implement and maintain complex business rules required for Health Benefits Exchange (HBE) and other systems in QHI. KY has selected Corticon BRE because of its ability to build, test, and deploy complex rules using its studio and its performance. Corticon also fits SOA infrastructure by deploying as a web service. KY considers the Corticon solution as scalable and having high availability.

   c. **Enterprise Service Bus (ESB):** KY has opted to use Microsoft BizTalk Server 2010 with its ESB toolkit 2.1 to provide a framework for integration of services. BizTalk's ability to build and deploy integration services for transforming and routing messages complements CHFS's existing Microsoft platform.

   d. **Security Framework:** The Kentucky Enterprise User Provisioning System (KEUPS) provides user provisioning and authorization services for all KY internal applications. Every component of QHI should invoke KEUPS services

prior to executing a user request including MEMS. KEUPS provides a single sign-on to most systems used by Workers and Citizens.

KEUPS integrates and synchronizes with the State's existing Active Directory as well as the State's mainframe security on the Z/OS. KEUPS provides support for claims aware applications via an Active Directory Federated Services (ADFS) based runtime authentication environment.

e. **Master Data Management (MDM):** Kentucky has opted to use IBM's Infosphere MDM (standard edition) for suites of master data management services. IBM's Initiate master data service is a comprehensive platform that enables rapid implementation of enterprise-wide master. It also delivers high-volume matching and linking through high-performance data processing and scalable database structures. The main purpose of MDM is to manage an Enterprise Master Person Index for KY citizens. The MEMS application should be required to register a person record with MDM to obtain an Enterprise Master Person Index (EMPI). MDM service should also maintain associated applications for each EMPI in its repository allowing easy correlation.

f. Data/Fraud Analytics Framework: KY has opted to use on-demand services of SAS Fraud Framework (SFF). These services should be hosted on the SAS network and QHI applications should access these services via ESB as well as via their dedicated portal. In addition to providing great value in the Medicaid arena, the additional modules of the SFF should be utilized by the Commonwealth to identify and prevent fraud, waste and abuse in many sectors, including areas like Medicaid, TANF, Child Care, and SNAP programs. SAS's predictive Analytics and Data Mining toolset should be utilized to accurately model our data to identify potential areas of savings as well as to help us to make evidence-based decisions.

g. Notification Fulfillment Service: KY has opted to implement customer communication service services to deliver notices, messages and documents through this shared service. KY is in the process of procuring HP Exstream to establish in-house comprehensive notification fulfillment service platform. KY plans to use this platform to deliver all communications on-demand or via batch, through multiple channels such as SMS, WEB, email, etc.

3. Applications:

a. **Kentucky Health Information Exchange (KHIE):** The KHIE is a fully functional health information exchange engaged with multiple small, medium, and large providers of healthcare data for the purpose of improving the quality and safety of healthcare in Kentucky. To accommodate the diversity of data sources in the health information exchange space, the KHIE has implemented a broad set of technologies to collect and consolidate clinical and claims-based data that are made available to exchange participants through web-

based technology or direct consumption. In addition, the KHIE supports the collection of healthcare data for secondary use such as the population of registries and public health surveillance systems. Exchange participants can share and retrieve data via peer-to-peer virtual private networks (VPNs) using Health Level 7 (HL7) messaging or by CCD-based web services exchange. Many participants are utilizing a combination of methods. The KHIE currently facilitates exchange for 125 distinct locations and 325 participation agreements have been executed representing more than 800 sites.

The KHIE is currently vendor-hosted, built on a .Net/BizTalk infrastructure. The master patient index is a Visionware Multiview implementation. The interoperability between KHIE and exchange participants (hospitals and provider practices) is built on standard IHE profiles. The KHIE is in the process of establishing Direct Exchange as defined by ONC to facilitate communication between health providers as well as between a provider and the KHIE.

b. **All Payer Claims Database (APCD)**: Following on Kentucky's implementation of ARRA, HITECH, and ACA health care reform and health information technology stimulus initiatives, the Commonwealth desires to move forward with implementation of an All Payer Claims Database (APCD). Access to timely, accurate data is fundamental to improving quality, mitigating costs, and promoting transparency in the health care delivery system.

   Kentucky's APCD is envisioned as a large-scale database including claims data derived from medical, eligibility, provider (physician and facility), pharmacy, and dental claims from private and public payers such as private insurance carriers (medical, dental, third party administrators (TPAs), pharmacy benefits managers (PBMs)) and public payers (Medicaid, Medicare).

   The APCD collects and provides information on inpatient, outpatient, pharmacy, and dental services for the commercially insured, publicly insured and self-insured populations. The goal is to provide true transparency across the spectrum of health care payers to create a foundation for actionable, accountable measures and to provide accurate information regarding the cost and quality of medical services so that residents of Kentucky are empowered to make well-informed health care decisions.

c. **Kentucky Department for Public Health (KDPH):** The mission of the Kentucky Department for Public Health is to promote and protect the health and safety of Kentuckians. KDPH provides policy and program governance for systems supporting local health departments, communicable disease control, disease and injury surveillance, enforcement of public health regulations, public health education, risk identification and reduction, policy development, and responses to disasters. A number of the programs use a

NEDSS Base System (NBS) implementation (i.e., to manage disease investigations and report infectious diseases to the CDC) and external partner systems should use the ESB to interoperate with the KY NBS. The Kentucky Immunization Registry (KY IR) is vendor-hosted and it is envisioned that registry data should be accessible through the Citizen Portal. The KHIE is currently exchanging data with the KY IR.

d. **Support Programs:** CHFS maintains number of application systems to support other Health and Family Services programs such as Child Support, Child Care, Children Welfare, etc. These application systems were developed and implemented having its own platform using mainframe, client/server and Web. Efforts are underway to modernize these systems as appropriate to utilize the QHI framework.

e. **Health Benefits Exchange (HBE):** The Commonwealth of Kentucky has contracted to develop a Health Benefits Exchange (HBE). The HBE is comprised of a closely integrated Eligibility and Enrollment (E&E) solution as well as a Plan Maintenance and Billing (PMB) solution. The HBE Vendor is in the process of implementing a custom E&E solution and COTS-based PMB solution. The core E&E system is being developed using Microsoft technologies. The E&E will be hosted at the Commonwealth's data center and the PMB will be hosted in a cloud environment by the Vendor.

   E&E is an end-to-end solution that includes functions required to process eligibility and enrollment for all Medicaid members (both Magi and Non-Magi) and other health insurance affordability programs offered on the HBE. It will also support functions such as workflow, Notifications, Scheduling, Document Management, Business Rules Management, and associated business processes required to launch and continuously operate an efficient and effective E&E System.

   A Plan Maintenance and Billing (PMB) solution includes functions required to offer and maintain individual and group insurance products including QHP Certification, Premium Billing, Collections & Reconciliation, Enrollment Maintenance, and more, required to offer individual and group health insurance products on the HBE and both support and sustain its seamless operation.

   Medicaid Eligibility is currently processed in Kentucky's legacy Kentucky Automated Management and Eligibility System (KAMES). KAMES also support casework and reporting functions for SNAP, TANF, and Medicaid programs. It operates on Commonwealth's IBM Z/10 model 2098-Q05 mainframe using CICS Transaction Server 3.2 and IMS DB control Version 9.1.

The HBE solution will be expanded to include functions for SNAP and TANF to replace the legacy KAMES system.

f. **Kentucky Medicaid Management Information System (KYMMIS**): The Kentucky Medicaid Management Information System (KYMMIS) is the current claims processing and retrieval system. The KYMMIS is hosted and maintained by Hewlett Packard Enterprise Services (HPES). KYMMIS is a customized rule based HP's interchange system. It supports both FFS reimbursement as well as Managed Care programs. The MEMS will replace the KYMMIS.

The Commonwealth utilizes .Net as its technology platform and strongly recommends that future applications employ this as well.

Medicaid modernization remains a high priority for the Commonwealth. It is seeking a partner that collaboratively works with stakeholders to develop a SOA and MITA-compliant enterprise system that utilizes sound technology, is flexible, and addresses current and future needs. The Commonwealth desires the system to be aligned with the CMS MITA current and future framework. The MITA Business Architecture should be reflected within the systems processes. The MITA Information Architecture should be reflected within the system's data models and information flows. The MITA Technical Architecture should be reflected within the SOA components of the system. It should include:

1. An SOA-based information system technical solution comprised of components that can be integrated into the Commonwealth's SOA framework or directly utilizes the Commonwealth's components.
2. A MITA-organized information solution that can be a single Vendor solution or a "best-of-breed" solution providing seamless integration of data from one MITA application area to another, one business process to another, across the enterprise
3. An information system that meets CMS certification requirements as defined in the CMS MECT for MMIS.
4. An information architecture and data management strategy that organizes, documents, and manages all of the data and enables easy access to information.
5. An information system solution that is flexible enough to fully support the administration of all of Kentucky's health care programs and can be easily configured to meet future expansion of programs and populations, and meet current and future regulatory needs.
6. The dynamic data exchange with external systems whenever possible and desirable. The system should support standards-based inbound and outbound transactions whenever appropriate.

Section 30.060.240.040—Service Oriented Architecture

The Commonwealth of Kentucky is expanding its vision of the MEMS beyond the scope of a traditional MMIS. The goal of the Commonwealth is to develop consumer-centric systems to provide the best services to the members of Kentucky combining efforts to streamline workflow, leverage all types of resources, and achieve economies of scale. The Commonwealth envisions a system that is adaptable, expandable, and flexible using the QHI architectural components wherever possible.

Section 30.060.240.050—Change Control

Changes in scope may happen due to a variety of unforeseen factors. For the purposes of this program, change is defined as a request originating from the Commonwealth that affects scope, schedule, and/or cost to the Commonwealth.

It is known, at the time of issuing of this RFP, that there should be changes to the requirements, presented herein, as rules and regulations evolve and are finalized by CMS and by the Commonwealth. These rules and regulations are expected to change through the life cycle of the project. Changes in requirements due to evolution of Federal and Commonwealth regulations do not constitute a change in scope for this program. Potential changes to regulations, such as those pending legislation or judicial review, that pose the potential to disrupt the delivery schedule should be documented by the selected Vendor in the Risk Log and managed accordingly.

The overall delivery dates, operational dates and quality criteria required by CMS and the ACA are not expected to change. If, however, CMS changes do affect delivery or operational dates, the selected Vendor adapts and responds to those changes. As part of Change Control Management, the Vendor documents formal change control process to be reviewed and approved by CHFS as part of the Program Management Plan. In the Program Management Plan, the Vendor should:

1. Describe both graphically (e.g., via a flowchart) and in text a recommended approach to change control, including steps, roles and responsibilities, and decision points.
2. Describe the Vendor's cost estimating steps and process for providing a written estimate to DMS of the cost and duration for every change. Vendor's estimates should meet at a minimum, 80% accuracy.
3. Provide sample change control forms and procedures the Vendor has used in other successful projects.
4. Agree that written approval by DMS is mandatory for every change before the Vendor begins development of that change.
5. Agree that written approval by DMS is mandatory for every change before the Vendor begins implementation of that change.
6. Agree in the proposed change control process that the Vendor should provide DMS with justification of every change suggested by the Vendor.
7. Agree that any changes be provided at a reasonable price to be negotiated between the Vendor and DMS, and that if the Vendor and DMS cannot come to an agreement on price and schedule to implement such mandated changes, the

Vendor agrees to perform the work at the price proposed by the State's project manager and to pursue the dispute resolution process to resolve open issues.

8. Identify and describe the Vendor's proposed tool(s) to track, manage, and report on change control items and to facilitate the Vendor's change control approach, including an automated tool that tracks history in a database. History should include the estimate and actual cost and duration for every change request as well as cumulative cost and schedule impacts for all changes for all periods DMS specifies.
9. Agree that the Vendor's proposed change control tools should be accessible by the Vendor, DMS, and DMS's designees.
10. Describe steps for updating the work plan for changes identified during DDI and approved by DMS.
11. Explain the benefits of the recommended change control approach for DMS.
12. Agree that the Vendor should meet all change control requirements throughout the term of the contract.
13. Agree that the Vendor's proposed change control process and tracking tool are subject to DMS approval.

The selected Vendor informs CHFS of any potential scope changes as soon as is reasonably possible to discuss, analyze, and document the impact of the change in scope, and determine direction and next steps. The assessment of the change in scope should include specific impacts to both schedule and costs. CHFS will work with the selected Vendor to confirm/reconfirm Project scope for subsequent activities, phases, and/or milestones. Additional details of the changes to scope are available in Section 40.050 and 40.055 of this RFP.

Section 30.060.250—Supporting Modules and System Components Outside the Core

The Vendor's MEMS solution should have the abilities to interact with other organizations or entities. Interactions should include the transmission of information through an interface for data population, verification or reporting. Third parties include the following organizations or entities: KHIE and CHFS.

Section 30.060.250.010—Web Services

The Vendor should include Web Portal solutions that provide communication, data exchange, and self-service tools to the provider community. The Portal should consist of both public and secure areas (web pages requiring a username and password). The public area should contain general information, such as program awareness, notices, and forms, and allow users to respond to surveys. Providers should have the capability of using a provider enrollment wizard, which includes the ability to track their application through the enrollment process. Other areas to be included in the portal are, but not limited to:

1. Perform provider enrollment and maintenance functions.
2. Inquire on recipient eligibility and enrollment.

3. Submit original claims, claim adjustments and prior approval requests.
4. Review claims payment and status information.
5. Access Prior approval requests.
6. Access State-approved forms.
7. Access provider training information including provider workshop registration, training materials, training evaluation forms, bulletins, broadcast emails, supporting documentation for training.
8. Enter registration to receive notifications and/or facilitate communications.

Section 30.060.250.020—Document Management System

Document Management provides the ability to view, capture, and attach scanned images to individual cases. The functionality includes the ability to link scanned and verified images to a customer that may exist in other systems.

The imaging/document management capabilities of the MEMS should include the ability to maintain current imaging files, provide users with access and retrieval functions and create any new imaging environment proposed to meet the functional requirements of this RFP. The contractor should convert historical images to the new environment and provide users with access and retrieval capability.

The Kentucky Access, Accuracy and Accountability Project (KAAAP) Electronic Case File system (ECF) is an existing Commonwealth system that was designed to serve as the Commonwealth's document management service. KAAAP ECF provides document management capabilities for various social and entitlement programs hosted in KAMES. The KAAAP ECF solution has been built on the SharePoint Platform, composed of SharePoint 2010, BizTalk 2010, SQL Server 2008 R2, MetaLogix Storage Point RBS File Share Provider, and Knowledge Lake Suite. Approximately 1.4M documents have been indexed using this solution post implementation.

The Commonwealth intends to enhance and modify the current ECF solution for incorporating the Document Management requirements of the MEMS. The enhanced ECF solution should provide standards-based integration services for interfacing with the MEMS solution. The Vendor's solution(s) should provide seamless interface for passing index values and other pertinent metadata from the MEMS solutions to the Document Management solution. The Vendor should be responsible for developing specific details of this interface during JAD sessions with the Commonwealth.

Section 30.060.250.030—Workflow Management

Workflow automation should use software to guide system users through various business activities which should be established for recurring sets of business operations that are done within the context of established procedures. The workflow software should retain all the artifacts, such as documents, e-mails, files, spreadsheets, and images within a centralized document/media management repository. The software should also capture the status of business activities and any administrative actions (approvals/disapprovals) collected along the course of any instance of a business

process controlled by workflow automation. The workflow software should be configured to enforce the established procedures or business rules related to the workflow, such as what documents are required, who needs to review and approve at each level, who needs to be notified of the progress, the routing and decision points along the workflow path, and the access to the workflow content based on the roles of the participants in the process. The use of workflow software should help to automate manual processes by integrating the documentation, generating notifications and alerts, scheduling and queuing work, and enabling electronic retrieval and status reporting. The workflow software should enforce standardization of the flow of business processes by ensuring routing, approvals, and content of each workflow in accordance with established business rules.

The MEMS should have the capability to set user defined system and personal alerts, such as ticklers and reminders. Alerts should be used for both internal staff and providers to provide notification of system changes, correspondence received, claim status, claim entry and routing processes, other user defined provider and client characteristics, and for monitoring activities and workflow. Alerts should consist of, but are not limited to, messages, documents, and images and should be supported by flexible routing, suspension, reminder and alert features.

Appendix K - Notifications to this RFP includes a preliminary list of the notifications that should be required. The selected Vendor should, prior to or during the System Design Phase, conduct discovery activities to compile a complete and final list of all notifications required to process life cycle management for all programs and products provided. The design and implementation of these notifications should not constitute a change in scope for this project. The Commonwealth is including a notifications system (HP Extream) as part of the HBE implementation and is hoping the MEMS Vendor should leverage usage of this system.

Section 30.060.250.040—Rules Engine

A rules-based solution should allow the Commonwealth to quickly implement policy and program changes and eliminate most of the hard coding in the back-end software programs. The proposed MEMS solutions should produce automated documentation of the current rules in effect as well as the history of all rules implemented.

CHFS has invested in the Corticon rules engine software for their HBE project and would prefer to leverage this in the MEMS; however, CHFS may consider other alternatives depending on the applicability of the solution.

CHFS requires business rules in both human- and machine-readable formats in order to submit to the HHS-designated repository in human-readable form so as to be made available to other states and to the public.

Section 30.060.250.050—Third Party Liability

The Vendor should propose a Third Party Liability (TPL) subsystem that is a fully integrated part of the MEMS solution. The TPL should obtain and utilize data from various sources to perform the following functions:

1. Identify third-party resources available to Medicaid members.
2. Identify third-party resources liable for payment of services rendered to Medicaid members.
3. Avoid State costs for these services.
4. Recover third-party funds.
5. Report and account for related information.

Section 30.060.250.060—Health Benefit Exchange

The Commonwealth is implementing an integrated multi-layer HBE solution that fulfills the certification requirements set out by the CMS and the Federal Government in response to the ACA.

The HBE solution is comprised of two separate but closely integrated solutions:

1. An end-to-end Eligibility and Enrollment (E&E) solution that includes functions required to process eligibility and enrollment for all Medicaid members (both MAGI and non-MAGI) and other health insurance affordability programs offered on the HBE, as well as supporting functions such as Workflow, Notifications, Scheduling, Document Management, Business Rules Management, and associated business processes required to launch and continuously operate an efficient and effective E&E System.
2. A Plan Maintenance and Billing (PMB) solution that includes functions required to offer and maintain individual and group insurance products including QHP Certification, Premium Billing, Collections & Reconciliation, Enrollment Maintenance, and more, required to offer individual and group health insurance products on the HBE and both support and sustain its seamless operation.

The Commonwealth's strategic vision is to extend the E&E solution to support additional human services programs including, but not limited to SNAP and TANF in subsequent phases of implementation.

Section 30.060.250.070—Immunization Registry

The Vendor's proposed MEMS should interact with the Immunization Registry providing data on a continual cycle. The interfaces should access the Registry through the KHIE. Data from the MEMS is critical to the overall effectiveness of the Immunization Registry. Its functionality would be hindered and ineffective if an interface did not exist between the Immunization Registry and the MEMS. This becomes apparent when such a registry is outside the domain of a Medicaid Department.

The data should help reduce the overall incidence of vaccine-preventable disease by giving providers and the Commonwealth a high-quality, confidential, flexible, and expendable tool. It would ensure age appropriate immunization for all children with the most efficient expenditure of the program and its resources.

Section 30.060.250.080—Customer Service Business Area

The Commonwealth intends to procure hardware, software and services for the implementation and operations of a Contact Center for the HBE that should provide customer support over the phone and on-line chat for various user types. This Contact Center will provide the technical infrastructure for the MEMS. The MEMS Vendor is expected to provide staffing support for Levels 1, 2, and 3 for providers and MCOs.

Vendor also maintains Help Desk staffing to provide users of ECM/EDI and MCO's with technical assistance and to provide users of electronic claim submission with technical assistance in accordance with Commonwealth-specified time parameters.

The selected Vendor should design and develop all codependent business process between the systems as well as all required APIs and web services. The selected Vendor should make available the necessary business and technical staff to participate in Contact Center interface and business process design to ensure a seamless integration. The Vendor should plan to provide staffing support for the Provider and EDI support.

Section 30.060.250.090—Pharmacy Benefit Manager

Pharmacy Benefit Management (PBM) is currently operated by a Third Party Vendor that uses the First Rx PBM System to provide Medicaid pharmacy services to approximately 124,000 members, over 3,000 pharmacies, and over 30,000 prescribers. The PBM processes pharmacy claims and manufacturer Rebates for the Commonwealth. The KYMMIS accepts, and ensures the integrity of, electronic pharmacy claim records submitted by the contracted PBM, including adjustments and reversals.

The proposed MEMS solution should support the interface(s) necessary to achieve bi-directional flow of information. The interface(s) should comply with the security framework of the Commonwealth, including existing Active Directory and mainframe security considerations and protocols.

Section 30.060.250.100—KEUPS

The Kentucky Enterprise User Provisioning System (KEUPS) is the Cabinet's security system. KEUPS is an identity management and single sign-on system that provides for centralized user management and includes functions for provisioning, de-provisioning, authentication, authorization, single sign-on, credentialing, and self-service and access audit/logging of the on-boarded CHFS applications. KEUPS should be utilized and integrated into the final systems design. KEUPS leverages .Net 4.0, SQL 2008 and ADFS 1.1.

The new MEMS solution should integrate with and utilize the CHFS security and enterprise user provisioning system, KEUPS for user registration, authentication,

authorization, provisioning and de-provisioning. In addition, users should utilize a common identity for a seamless single sign-on experience.

Section 30.060.250.110—Medicaid Waiver Case Management System

The mission of the Division of Developmental and Intellectual Disabilities (DDID) within the Department for Behavioral Health Developmental and Intellectual Disabilities (DBHDID) is to empower each person to realize his or her place in the community as a citizen of the Commonwealth of Kentucky. To accomplish this mission, DDID partners with and supports persons with intellectual or developmental disabilities, families, advocates, stakeholders and government agencies. The Medicaid Waiver program uses a combination of Federal and State funding to provide services and supports in the community for individuals who meet the level of care criteria for institutionalization.

DDID provides an array of supports for individuals with developmental and intellectual disabilities. This is accomplished through contracting for services through the fourteen (14) Regional Mental Health/Mental Retardation Boards and other qualified private providers. Services funded by DDID are provided in varying degrees by each of the Regional Boards (a.k.a., Community Mental Health Centers) and their affiliates. These services include case management, residential, vocational, respite, crisis intervention, leisure and recreation, in-home support, and habilitation.

The current process of oversight of providers and collection of information regarding individuals receiving services is a combination of paper processes, email, and numerous databases. The nature of the current processes is cumbersome, inefficient, duplicative, and hosts the opportunity for numerous errors and data integrity issues. The manual process also poses many challenges when changes to the required forms or the process itself are needed. Lastly, the current process makes it very difficult to track health and safety trends and to provide the necessary reports as required by CMS.

DDID is publishing an RFP in the near future seeking a comprehensive web-based level of care and case management solution to support functionalities for all user bases including clients, State staff, and providers. It should meet the needs of DDID's business processes, including applicable State and Federal requirements. The MEMS should interface with the Waiver Case Management System.

Section 30.060.260—Options to Buy

Throughout the Scope of Work, the Commonwealth has maintained the necessity to comply with the CMS Seven Conditions and Standards. Modularity presents the opportunity to identify areas of the MEMS solution as "Options to Buy." These areas may or may not be exercised within the contract. Proposed solutions for each "Option to Buy" along with individual component costs detailed in Section 70 will assist the Commonwealth in meeting CMS standards. The "Options to Buy" are identified below:

Section 30.060.260.010—Systems Hosting, Operations and Disaster Recovery Activities "Option to Buy" (Section 60.010.010.150)

The successful Vendor performs operations and maintenance throughout the life of the contract at no additional cost to the Commonwealth to include the following:

1. Data center operations.
2. Updates, patches, and repairs to components of the production, test and all other accessible environments, including, but not limited to:
   a. Hardware.
   b. Operating systems.
   c. Database systems.
   d. Utilities for systems, database, software, communications.
   e. Voice, video, data communications lines.
   f. Communications software.
   g. Drivers.
   h. Configurations.

Section 30.060.260.010.010—Infrastructure Hosting

The Commonwealth is interested in maximizing its efficiency by exploring all available infrastructure hosting options for the MEMS solution. This includes the possibility of using the Commonwealth's existing Data Center in COT or a Vendor-provided cloud-based infrastructure. CHFS requires a plan to provide all hardware and software required for development, test, implementation, production operations, and disaster recovery site operations for the MEMS solution.

The Vendor assumes responsibility for installing and configuring the necessary hardware and software with the appropriate coordination of COT. The support from COT should include areas such as network and security access to the Commonwealth network, building/facility access, data farm and server room access on as-needed basis, shared BizTalk environment access, and file server access. The schedule for the installation and setting up of various environments should be mutually agreed and finalized in the work plan. All hardware and software should be implemented and appropriately configured by the selected Vendor in the environment prior to the start of the relevant phase based on the schedule in the project work plan.

For details on the Commonwealth's infrastructure requirements, the Vendor should reference Section 30.060.240.010 of this RFP.

Section 30.060.260.010.020—Maintenance Services

The Vendor performs software and hardware maintenance for the component parts of the MEMS implementation, as directed by the Commonwealth. It is the Commonwealth's expectation that all maintenance requirements be accomplished

under the terms of the contract's firm fixed price for ongoing operations, including machine time, person time, documentation support and any other related support.

Section 30.060.260.010.030—Disaster Recovery & Business Continuity

The Vendor should create and maintain a Disaster Recovery Plan (DRP) to include back-up procedures and support to accommodate the loss of online communication between the MEMS Vendor's processing site and Commonwealth facility(ies) in Kentucky; disasters or occurrences which cause a disruption to the processing of Kentucky transactions (claim records, eligibility verification, provider file, updates to the MEMS, and so forth); loss of the Vendor's primary processing site; or loss of access for the Commonwealth online component of the MEMS.

The Vendor must maintain a CHFS approved BCP Plan and Disaster Recovery and System Back-up Plan at all times. It is the sole responsibility of the MEMS Vendor to maintain adequate backup to ensure continued automated and manual processing. The Plan must be available to CMS, CHFS, or State auditors at all times. All critical operations must be clearly defined in the MEMS Vendor's CHFS approved disaster recovery plan and must resume in no later than five business days following a disaster.

The KYMMIS Vendor must provide an alternate business area site in the event the primary business site becomes unsafe or inoperable.

The Vendor should propose a plan inclusive of the items required to operate an alternate disaster recovery site for the continued operation of the MEMS solution in the event of a disaster. The Vendor should provide options for recovery within 24 hours, 48 hours, 72 hours and120 hours of the disaster event. This "hot" disaster recovery site should be built, configured, and maintained by the Vendor. The Vendor should include in its plan a description of all services, hardware, software, software licenses, and infrastructure required for this functionality. The alternate site should be configured to the same system performance specifications as the primary hosting site for all systems in the MEMS.

Section 30.060.260.020—Decision Support System –"Option to Buy" (Section 60.010.010.160)

The replacement Decision Support System (DSS) should take advantage of the advancements in system architecture and Web technologies to provide an economical and flexible data storage system. The DSS should integrate seamlessly with the MEMS and take advantage of system interoperability and interface technologies. The Vendor should take into consideration the needs of the less technical user as well as the more sophisticated user and provide a solution to meet the informational needs of the Commonwealth at all levels.

The DSS should function as a data storage repository for recipient, provider, claim, reference and encounter data, and data sets from external sources that may be

designated by the Commonwealth. The Vendor should provide a DSS with sufficient space and planning for efficient operations and growth throughout the life of the contract.

All hardware and storage space required to house the data should be included in the contract, purchased and maintained by the Vendor. At termination of the contract, the hardware becomes the property of the Commonwealth.

In addition, the DSS should:

1. Maintain data sets approved by the Commonwealth for all tables, including provider, recipient, claims, encounters, and reference:
    a. Implement a data model that is flexible and allows for the addition of new data elements with minimal effort.
    b. Include all necessary data elements to perform all business functions described in this RFP.
    c. Maintain the most recent seven (7) years of paid and denied claims and encounter data.
    d. Maintain all purged prior years' claim and encounter data in a separate file or files for ad-hoc reporting. Each year should be maintained on a separate file to allow the query of the data as it was at the end of the reporting year.
    e. Maintain a minimum of seven (7) years of recipient historical eligibility and claim information in order to track changes in a recipient's health status over time.
    f. Maintain risk-adjusted data based on the most recent two years of eligibility and paid claims.
2. Integrate robust user-friendly query, analysis, and reporting tools and functionality including:
    a. Provide sufficient processing/storage for the creation of reports and statistics by State staff, a minimum of 2.5 Terabytes at the beginning of the contract and increasing each year if necessary based on utilization statistics.
    b. Support a variety of output capabilities including CD, DVD, tape, FTP and other methods as determined by the Commonwealth.
    c. Provide the functionality to allow authorized State users the ability to link between Contractor tables and user-defined tables as necessary.
    d. Provide the ability for certain State users to retrieve data from any DSS table via ODBC and other available database interfaces.
    e. Provide Web-based access to DSS functionality.
    f. Provide reliability, stability, and recoverability.
3. Support all users authorized by the State:
    a. Support at least 600 named users of the DSS.
    b. Support at least 200 average users each week.
    c. Support users at Area Offices, headquarters, other State agencies, and other locations authorized by the State.

Additional Functional Requirements can be found in Appendix A – MEMS Functional Requirements, DSS tab.

Section 30.060.260.030—Utilization Management Module–"Option to Buy" (Section 60.010.010.170)

Medicaid modernization remains a high priority today for the Commonwealth. Advances in HIT, including the deployment of EHRs, HIEs, and the need for interoperability across systems to support patient safety and quality of care, are driving forces in health reform and other efforts to improve care and reduce unnecessary costs. Alignment with national health initiatives, such as the Nationwide Health Information Network (NHIN), makes the potential for using business data to develop performance metrics for evaluating health outcomes at all levels of health care delivery systems extremely viable.

In support of Medicaid modernization, CHFS is seeking a robust Utilization Management (UM) program to ensure Medicaid members receive safe, quality health care while simultaneously reining in costs for medically unnecessary care. DMS seeks to continue to reduce medically unnecessary care and improve outcomes through a state-of-the-art UM Module. The module should help ensure that Medicaid spending supports clinically appropriate care, improved patient safety, and quality of care.

The UM module should provide statistical information on members and providers enrolled in the Kentucky Medicaid Program. The module should include effective algorithms for isolating potential misuse and produce an integrated set of reports to support the investigation of that potential misuse.

The UM module should provide extensive capabilities for managing data summarization, exception processing and report content and format. Parameter controls should allow the user to limit the volume of printed material required for analysis. Parameter-driven data selection, sampling, and reporting features would further enhance the capabilities of the module.

The module should have the capability to produce comprehensive profiles of the delivery of services and supplies by Medicaid providers and the use of these services by Medicaid members. Both summary and detail claim data should be available to the reviewer, who is able to control the selection of claims and content of reports through parameters. Statistical indices should be computed for selected items to establish norms of care so that improper or illegal utilization can be detected.

The Vendor, or subcontractor, should meet the flowing requirements:

1. Be Designated as a Quality Improvement Organization (QIO) or QIO-like entity by CMS for a minimum of the past five (5) years.
2. Be Accredited by Utilization Review and Accreditation Committee (URAC) in Health Utilization Management or National Committee of Quality Assurance (NCQA) in Utilization Management.

3. Have worked as a Medicaid Utilization Review Organization for at least the past three (3) years, including performing waiver, LTC, and EPSDT utilization review services.

Functional Requirements can be found in Appendix A – MEMS Functional Requirements, Utilization Management tab.

Section 30.060.260.030.010—Implementation Requirements

CHFS expects that the Vendor follows a standard SDLC for the DDI period. The Vendor should create comprehensive plans, with CHFS approval, prior to undertaking all facets of the development and implementation of the module. The project work plan should be logical in sequence of events including appropriate review time by CHFS and sufficient detail for review. The plans should include a narrative that provides an overview of the approach that should result in an orderly transition of responsibilities. It should encompass all activities necessary to assume the responsibilities as the Medicaid UM Vendor in addition to a back-up and disaster recovery plan.

The Vendor should submit a written report of program progress to CHFS every week. The progress report should specify accomplishments during the report period in a task-by-task format, including personnel hours expended, whether the planning tasks are being performed on schedule, and any administrative problems encountered.

Section 30.060.260.030.020—Utilization Management Project Staffing

At all times during this project, the Vendor should have the adequate number of project staff members necessary to ensure successful implementation. The Commonwealth should provide a limited number of full-time staff members, located at the Commonwealth, who are dedicated to providing oversight and assistance during the project.

All project staff members shall sign all CHFS forms related to such items as disclosure of information, security, acceptable use of equipment, etc.

The Vendor provides the equipment, software, and tools necessary for the Vendor's project staff members. Any personal computers or equipment connected to the Commonwealth network should conform to CHFS minimum configuration requirements. All Vendor IT equipment connected to the Commonwealth private network should have the standard CHFS image and security policy applied. All equipment should be sanitized prior to removal from service on the CHFS network.

Section 30.060.260.030.020.010—Utilization Management Project Manager

The Vendor should provide a dedicated full-time Project Manager who begins project work on the negotiated start date following the contract award, and continues that work until the Commonwealth provides the Vendor with a written acceptance of completion of the project. The Commonwealth may require replacement of the Project Manager for any reason. The replacement should be approved by the Commonwealth.

The Project Manager leads the development and daily management of the project, and be responsible for overall Vendor performance, quality of deliverables, and contract compliance for the duration of the contract. The Project Manager should be located with the project team and is the primary point of contact with the Commonwealth, responsible for the management and communication of project tasks, deliverables, schedule, issues, and risks. The Project Manager is also responsible for all Vendor subcontractor work and products.

Section 30.060.260.030.020.020—Utilization Management Staffing Requirements

The Vendor provides qualified staff to meet an appropriate staffing level to satisfy the requirements specified in this RFP and the resulting Master Agreement. The Vendor should, at a minimum:

1. Create and maintain a DMS-approved staffing plan that demonstrates the ability to ensure employment of qualified staff.
2. Hire and retain qualified staff to perform UM functions.
3. Employ the following key personnel:
    a. Project Manager as, detailed in Section 30.060.280.020.020.010.
    b. Medical Director for Physical Health to oversee utilization review process and peer consultant network.
    c. Medical Director for Behavioral Health to oversee behavioral health review process and Behavioral Health peer consultant network.
    d. Training and Outreach Manager to oversee all training and outreach activities.
    e. Qualified Mental Retardation Professional, with a minimum of three (3) years of recent experience working with mental retardation, to support the SCL program.
    f. EPSDT Coordinator with a minimum of five (5) years of recent experience working with EPSDT, to provide oversight for the EPSDT Special Services program.
4. Provide a team of experienced clinical and physician reviewers, with a minimum of three (3) years of recent experience, to perform medical necessity reviews.
5. Provide a team of experienced Behavioral Health utilization reviewers with a minimum of three (3) years of recent experience, to perform Behavioral Health and Impact Plus reviews.
6. Provide a team of experienced EPSDT utilization reviewers, with a minimum of three (3) years of recent experience, including experience with children and adolescents with severe emotional disabilities and substance abuse, to perform EPSDT and Impact Plus reviews.
7. Provide a team of experienced Medicaid Waiver utilization reviewers, with a minimum of three (3) years of recent experience, to perform Waiver reviews.
8. Provide a team of experienced long-term care utilization reviewers, with a minimum of three (3) years of recent experience, to perform Nursing and ICF/MRDD reviews and audits.
9. Recruit and maintain an adequate network of peer consultants.

10. Ensure that all administrative reviewers possess at least one (1) year of recent medical utilization review experience.
11. Provide staff with initial and ongoing training that, at a minimum, covers the following topics: utilization review policies and procedures, medical necessity criteria, and Master Agreement requirements.
12. Ensure that all physician and clinical reviewers meet and maintain qualifications required in State and Federal regulations, including appropriate licensure.
13. Ensure staff know and abide by KY guidelines when sending children and adolescents out of state for psychiatric residential treatment. Staff should be familiar with all in-state psychiatric facilities and programs.

Section 30.060.260.030.030—Utilization Management - General Operations

The Vendor should perform the responsibilities described in this RFP and in the Appendix A – MEMS Functional Requirements (Utilization Management Tab) and Appendix B – MEMS Technical Requirements.

The Vendor is subject to monitoring and evaluation by DMS as set forth in 42 CFR 456 – Utilization Control. The Vendor is required to adhere to the performance requirements of the Master Agreement as well as the requirements of any revisions in Federal and State legislation or regulations which may be enacted or implemented during the period of performance of this Master Agreement that are directly applicable to the performance requirements of this Master Agreement. Such requirements should become a part of this Master Agreement effort through execution of a written contract amendment.

Section 30.060.260.030.030.010—Utilization Management Requirements

The Vendor should demonstrate high quality administrative and clinical leadership in UM services. The requirements in this section are applicable to all review functions. The Vendor's general requirements include, but are not limited to the following:

A. Evaluation of Utilization Management Program

Complete an initial and annual UM evaluation that includes a UM work plan and targeted return on investment (ROI) projections.

B. Utilization Management Policies and Procedures

Develop, publish and maintain a DMS-approved UM manual that includes policies, procedures and workflows. The manual should be updated as needed, but no less than on an annual basis.

C. Utilization Review Committee

Establish and maintain a Utilization Review Committee with DMS participation to provide oversight of the UM function.

D. Peer Consultant Network

Develop and maintain a network of peer consultants to assist, at a minimum, in:

1. Addressing medical necessity determinations.
2. Researching new technology.
3. Developing medical policies.
4. Addressing quality issues.
5. Supporting the appeals and hearing process.
6. Reviewing health care issues referred by DMS.

E. Outreach and Training

Create and maintain an Outreach and Training program for UM. At a minimum, the program should include:

1. DMS-approved training plan that identifies the training needs during project, development, implementation and operational phases.
2. DMS-approved outreach plan, which at a minimum, includes written communication, telephonic communication, web communication, focus groups, webinars, and "live" face-to- face training for all aspects of the UM program.
3. DMS-approved work plan to specifically address methods to increase web submission of utilization review requests. It is expected that the Vendor receives no less than 50% of non-waiver utilization review requests by web submission at end of year one. Increases are expected beyond year one based on a DMS-approved target for each year.
4. Development and maintenance of DMS-approved educational materials that address the utilization review process.
5. Initial and ongoing seminars to educate providers on the utilization review process.

F. Reconsideration and Appeals & Hearings

1. Make a determination to uphold, modify, or reverse the denial of requested services. The physician handling the reconsideration should be different than the one that performed the initial review.
2. Support administrative appeals and hearings by reviewing and submitting requested clinical information, preparing case summaries and providing testimony regarding the utilization review process.

G. Audits, Meetings and Facility Reviews

Perform UM audits, including reviews for Reserved Bed Days and Utilization Programs of Facilities.

H. Internal Quality Control Program

Develop and implement an Internal Quality Control Program to ensure appropriate administration of all responsibilities.

I. Reporting

1. Establish and maintain a system to produce accurate, timely, and complete periodic (daily, weekly, quarterly, and annual) and ad hoc reports that, at a minimum, depict:

2. Overall performance of utilization review activities for all type of services (e.g., EPSDT, durable medical equipment, waiver services), including type of reviews, volume of reviews, disposition of reviews, and processing time.
3. Overall performance of customer service activities, including, abandonment rates, average speed of answer, volume of inquiries, type of inquires, and rate of requests received by web submission.
4. Utilization patterns of providers and members.
5. Utilization patterns based on geographic region and type of service.
6. ROI or savings on administrative and clinical utilization initiatives, such as those identified in the Evaluation of the UM Program.

Section 30.060.260.030.030.020—Utilization Review Requirements

1. Perform prospective, concurrent, and retrospective review of DMS services.
2. Make Medical Necessity Determinations of whether a covered benefit or service is medically necessary.
3. Utilize criteria to determine if a covered Medicaid service or benefit is clinically appropriate.
4. Perform utilization review.
5. Require a licensed physician to make utilization review decisions related to denials, reductions, or limitations.
6. Provide an automated rule driven system-based review process through which providers have 24x7x365 access to submit both initial and concurrent requests and clinical information and obtain real-time approvals.
7. Provide a Customer Relations Management Service (CRMS) which includes the ability to communicate to inquiries, requests and complaints via telephone, email, fax, web or mail.
8. Report, in a format approved by DMS, suspected fraud and abuse identified during reviews, audits, on-site reviews, or any other communication, within timeframe defined by DMS.
9. Perform prior authorization for FFS members.

Section 30.060.260.030.030.030—Utilization Management System Requirements

The Vendor has the necessary technology needed to fully manage and report on the utilization management program described in this RFP and resulting Master Agreement. The Vendor should, at a minimum, provide the following:

1. The Vendor should provide a proven and reliable automated, rule driven web-based utilization management system for receiving, collecting, transmitting, and routing utilization management requests. This system should fully interface with the current and any future MMIS. The Vendor should, at no additional cost, coordinate with the State's FA to ensure a timely and fully functioning interface with the MMIS.
2. The Vendor should produce system-generated periodic (daily, monthly, quarterly, or as otherwise requested) reports. The system should also be able to produce ad hoc reports.

3. The system should generate unique PA numbers to all PA requests immediately upon receipt, and maintain all PA data on the PA file, regardless of disposition.
4. The Vendor should ensure that only valid data is entered on the PA file and deny duplicate requests or requests that contain invalid data.
5. The system should capture and maintain both the requested service amounts (units and/or dollars) and authorized service amount (units and/or dollars) on the PA file.
6. The system should authorize services for a specific recipient, at a minimum, by procedure codes, diagnosis codes, types of service, units, dollars, origin, destination, provider number, and provider types.
7. The system should track modifications to authorization records (i.e., partial approval and partial denial on the same authorization record, appealed authorization upheld and modified, etc.) and maintain a DMS-approved audit trail of file updates.
8. The system should have the capability to change the services authorized and to extend or limit the effective dates of the authorization. Additionally, the system should also maintain the original and updated data in the authorization records.
9. The system should have the capability to inquire/access/report the prior authorization.
10. The system should provide the capability for providers to submit and check the status of PA requests.
11. The system should provide the capability for authorized DMS staff to check the status of all PAs.
12. The Vendor should use imaging equipment to capture, store, and retrieve hard copy authorization requests and associated documents and enter these requests to the on-line authorization system. Documents need to be electronically linked to the appropriate prior authorization request.
13. No less than 24 hours of an utilization review determination, the Vendor should generate and send to the appropriate requesting and/or rendering provider(s) and recipient a DMS-approved notice of disposition (approval, denial, reduction of service). The Vendor should maintain electronic copies of the notification letters to be provided to DMS within one (1) business day of request.
14. The Vendor should accurately and timely implement into its systems and processes all known (i.e., ICD-10, Version 5010) and future CMS and other Federal and State mandates.
15. The Vendor should provide fully tested connectivity to the current fiscal agent's existing system.

Additional Functional Requirements can be found in Appendix A – MEMS Functional Requirements under the Utilization Management tab.

Section 30.070—Takeover of Current KYMMIS

The Scope of Work (SOW) for the KYMMIS Takeover Project provides the information necessary to understand taking over the Medicaid services, systems, and operations that is the KYMMIS. The Vendor awarded a Contract must provide management plans

to identify timelines, provide sufficient resources (including qualified staff), define processes, and identify standards to accomplish all of the tasks contained in this RFP.

Section 30.070.010—IdentityTheft Prevention and Reporting Requirements

The selected Vendor is responsible any mitigation, cleanup and reporting costs from Identity Theft, system breach or breach as defined under the HIPAA Privacy Rule. For even a single knowing violation of these Identity Theft Prevention and Reporting Requirements, the vendor agrees that the Commonwealth may terminate for default the contract(s) and may withhold payment(s) owed to the Vendor in an amount sufficient to pay the cost of notifying Commonwealth customers of unauthorized access or security breaches. The Vendor must attest/certify to KYMMIS that it has established and will share a breech notification policy and program.

Section 30.070.020—Security

The Vendor should adhere to the Commonwealth Office of Technology (COT) security and enterprise policies and procedures and the CHFS security policies and procedures.

1. COT Enterprise policies can be viewed at http://technology.ky.gov/governance/Pages/policies.aspx
2. COT Security Procedures can be viewed at https://gotsource.ky.gov/docushare/dsweb/Get/Document-329691
3. CHFS Security Policies are available at http://chfs.ky.gov/os/oats/policies.htm

Section 30.070.020.010—Security Services

1. NIST baseline should be moderate.
2. Provide annually a SSAE 16 (or comparable review) to the Cabinet for Health and Family Services (CHFS) for the Frankfort office location of the selected vendor. The data center where the system is hosted must also provide an annual SSAE 16.
3. The Vendor must perform a Risk Assessment following HIPAA guidelines every 365 days
4. Security Testing is required by the selected Vendor on functional, technical and infrastructure components to ensure the system meets all system security requirements. Security Testing scenarios and strategy shall be approved by the CHFS Information Security Office (CHFS ISO) prior to execution and all Security Testing results shall be approved by CHFS and CHFS ISO. Additionally, the selected Vendor is required to conduct its own security risk assessment prior to the Commonwealth engaging a Third Party Vendor to conduct the Independent Security Assessment. The selected Vendor shall provide a report of the results of its security risk assessment, including all tools used, such as code scanning and application scanning tools, and an action plan of remediation for vulnerabilities

identified. The Vendor should have a third party security assessment done annually as required by CHFS/COT Policies.

5. The Vendor shall establish and maintain appropriate levels of disaster recovery and regularly test the established disaster recovery. The Vendor should discuss options available as part of the solution related to disaster recovery. It is the preference of CHFS that this include local hot swap/hot fail over redundancy in all critical components as well as hot site operations with database replication.

Section 30.070.020.020—Security Plan

The Security and the Privacy Impact Assessment should be included as a separate document.

1. Provide a detailed in-depth data flow diagram of the KYMMIS system illustrating the security mechanisms.
2. Provide a detailed in-depth architectural diagram for the KYMMIS system to include all infrastructure.

Section 30.070.020.030—HIPAA Compliance

The KYME is compliant with HIPAA rules for access, authentications, storage and auditing, and transmittal of electronic personal health information (e-PHI). Standards include HIPAA Version 5010 standards for electronic health transactions (effective January 1, 2012) are currently in effect.

The selected Vendor should comply with the KYME HIPAA compliance controls and procedures and should submit updates to the plan for CHFS for review and approval.

The selected Vendor is not permitted to use or disclose health information for any reason other than that mandated within this RFP.

Section 30.070.030—Takeover Activities

The activities to transition to a new KYMMIS Vendor begin on the effective date of the Master Agreement. Takeover includes the activities required to successfully transfer, configure, install, test, and implement KYMMIS for the Commonwealth and assume responsibility for its ongoing operations and maintenance.

The KYMMIS Vendor should conduct a detailed survey and analysis of the current KYMMIS, including the operation and maintenance of the KYMMIS, current procedures, work in progress, outstanding work, and user requirements in finalizing the WBS required as part of the Vendor's technical proposal.

The KYMMIS takeover activities should include, but not be limited to, processing tests and an operational readiness review sufficient to demonstrate that the KYMMIS Vendor is ready to begin operations for each and every function.

DMS must approve the KYMMIS Vendor's operational readiness test before the initiation of the KYMMIS production operations. In the event DMS does not approve the start of the KYMMIS Vendor's production operations, the Vendor shall be responsible for making arrangements to continue the FA operations. The KYMMIS Vendor will operate and maintain a Federally-certified MMIS. The KYMMIS Vendor shall be liable for damages incurred by the Commonwealth.

Additionally, DMS plans to contract the services of an IV&V Vendor. The IV&V Vendor validates that the KYMMIS Vendor has supplied an acceptable product and performs verification activities to check that system and operational services meet design requirements, specifications, and regulations.

Section 30.070.040—Project Organization (See Section 60.020.010.050) (125 Points)

A major factor in the success of this project will be the degree of collaboration between the KYMMIS Vendor and the Commonwealth Project Management Office. In recognition of this, DMS has established a governance system consisting of an Executive Steering Committee and a Project Director level Change Control Board (CCB) for overall project change control.

The Project Change Control Board is comprised of a subset of individuals from the Executive Steering Committee along with the Project Director. It is charged with the governance of the project in the following areas:

1. Change Management.
2. Risk Management.
3. Issue Management.
4. Action Item Management.

DMS staff will participate directly in project management, requirements validation, design, development, testing, and transition of the Takeover. Additionally, DMS has established the appropriate levels of management oversight to monitor project progress and assess Vendor performance for each project phase.

The Takeover Vendor will support the IV&V Contractor in its objective verification and validation activities. The IV&V Contractor will have access to all deliverables and visibility into the Takeover Vendor's processes to produce those deliverables.

Section 30.070.040.010—Project Governance

Project governance helps ensure that a project is executed according to the standards of the organization performing the project. Governance keeps all project activities above

board and ethical, and also creates accountability. A project governance structure will also help define a project reporting system. It outlines specific roles and responsibilities for everyone involved in the project.

Project Governance for the KYMMIS Takeover Project will be maintained through two avenues; a Steering Committee made up of Commonwealth leadership, and a Project Management Office (PMO) office. The Steering Committee will provide direction and guidance for the entire project.

Section 30.070.040.020—Commonwealth PMO

The Commonwealth will implement a PMO under the Project Governance structure for the KYMMIS Takeover Project. The Commonwealth PMO will define and maintain the standards for the project.

Section 30.070.040.030—Project Management Approach

The entire project will be managed according to industry best practices outlined in the Project Management Body of Knowledge® (PMBOK). A Project Management Plan (PMP) outlining scope, schedule, and cost will be developed with DMS to guide the management of the project. In addition, a Communication Plan, Risk Management Plan (RMP), and Quality Management Plan (QMP) will be used to ensure successful delivery of a quality takeover that will continue to meet CMS MMIS certification standards, and the KYMMIS Testing Plan will provide guidelines for testing all types of updates to the KYMMIS. During the startup of this project, DMS and the KYMMIS Vendor shall outline all plans necessary for the KYMMIS. The KYMMIS Vendor shall follow and update all applicable plans throughout all phases of the project. The IV&V Contractor will work closely with the Commonwealth PMO to ensure a successful project.

Section 30.070.040.040—Deliverable Review Process

Copies of each deliverable, as defined in the approved work plan, must be delivered to DMS in final form, in the number specified, and on the date specified in the work plan. DMS requires an electronic copy of all deliverables. The electronic copy must be compatible with MS Word or other application software as requested by DMS. All deliverables must be in a format approved by DMS and meet content requirements specified or as subsequently defined by DMS.

DMS will have 10 working days to review each deliverable outlined in this RFP and will either notify the KYMMIS Vendor of acceptance or will provide a detailed list of deficiencies that must be remedied. In the event that DMS notifies the KYMMIS Vendor of deficiencies, the KYMMIS Vendor shall correct the deficiencies within five working days, unless DMS consents in writing to a different timetable.

All project management deliverables, as listed in Section 30.070.030, must be delivered in draft form within the vendor's proposal. After signing of the Master Agreement, the KYMMIS Vendor will deliver updated plans to DMS within 20 working days of the effective date. The KYMMIS Vendor shall conduct a walkthrough, at DMS request, to ensure complete understanding of the products and plans by all involved.

Section 30.070.050—Project Kickoff

During the Initiation Phase, the Commonwealth PMO will conduct a Project Kickoff meeting prior to the startup of activities. The PMO will identify project stakeholders and hold this meeting in order to convey the project goals, project structure and plan, project timeline, and stakeholder roles in the project.

Section 30.070.050.010—Project Management Vendor Deliverables

This section contains the project management deliverables, consisting of:

1. Staffing Management Plan.
2. Communication Management Plan.
3. Schedule/Work Breakdown Structure.
4. Takeover Management Plan.
5. Risk Management Plan.
6. Quality Management Plan.
7. Change Management Plan.
8. Business Continuity Plan.
9. Disaster Recovery Plan.
10. Training Plan.
11. Testing Plan.
12. Hardware/Software Configuration Plan.
13. Configuration Management Plan.

Section 30.070.050.010.010—Staffing Management Plan

The Staffing Management Plan will contain project staff, project staff roles, project staff resumes, a project team experience matrix and organizational charts with defined responsibilities, and contact information. Resources must be allocated by name or by type to the Work Breakdown Structure (WBS). Staff allotted to the project must remain for the duration of the project unless changes are authorized by DMS.

The Vendor is responsible for updating the Staffing Management Plan as necessary and throughout all phases of the project until the end of the contract period.

Section 30.070.050.010.020—Communications Management Plan

The Communications Management Plan will incorporate processes to ensure timely and appropriate generation, collection, distribution, storage, and retrieval of project information. The Communications Management Plan ensures that the correct individuals receive required information in a timely manner.

The Vendor is responsible for updating the Communications Management Plan as necessary and throughout all phases of the project until the end of the contract period.

Section 30.070.050.010.030—Schedule/Work Breakdown Structure

The Schedule/Work Breakdown Structure will be the result of scope planning and scope definition tasks and will be created in Microsoft Project or a format approved by DMS. The WBS will be updated on a bi-weekly basis and at a minimum, must include:

1. Key dates, and dates for submittal of deliverables.
2. Structure, using a breakdown of task, sub-task, and activity work steps within each of the major Design, Development, Testing, and Implementation (DDI) phase activities:
    a. System design.
    b. System development/testing.
    c. Data conversion, if needed.
    d. UAT and implementation.
    e. Operations.
3. Description, at the sub-task level, which includes:
    a. Personnel resources applied by name and level of effort, in hours.
    b. CHFS resource requirements (personnel and other).
    c. Duration of task.
    d. Dependencies.
    e. All required deliverables.
    f. Gantt chart.
    g. Program Evaluation and Review Technique (PERT) or dependency chart.
    h. Resource (personnel and other) matrix by sub-task, summarized by total hours by person, per month.

Section 30.070.050.010.040—Takeover Management Plan

The Takeover Management Plan will address the Commonwealth's desire to reduce risk during takeover and implementation of the systems. The new KYMMIS Vendor shall receive and install a copy of the KYMMIS provided by the incumbent. The new KYMMIS Vendor must install the KYMMIS at its facility and must demonstrate completeness of the takeover, including any KYMMIS system changes subsequent to receipt. Takeover of the FA operations will be a critical process for the overall success of the project.

The new KYMMIS Vendor must successfully plan for and perform the KYMMIS Takeover and implementation. The new KYMMIS Vendor will implement the current KYMMIS on its own hardware, installing all software and the telecommunications networks required to operate the system according to the specifications outlined in the current system documentation which can be found in Section 20.010.11–Procurement

Documentation and the Master Agreement. The Vendor will produce or develop any software solutions necessary to perform its operational responsibilities, in the event one does not exist (e.g., data entry, claims control, electronic claims submission software, change control tracking system). The Vendor shall provide parallel facilities for disaster recovery and testing of the system.

Section 30.070.050.010.050—Risk Management Plan

The Risk Management Plan will, at a minimum, address the process and timing for risk identification, describe the process for tracking and monitoring risks, describe the governance structure involved in and procedures for identifying and reporting potential risk and risk resolution, identify the tools and techniques that will be used in risk identification and analysis, describe how risks will be quantified and qualified, and how risk response planning will be performed.

Reporting of risks will be in an approved format, including but not limited to:

1. A brief written evaluation of each risk and potential impact.
2. Setting a risk ranking or risk priority based on likelihood of occurrence.
3. Assignment of risk management responsibility.
4. Creation of a risk mitigation strategy.
5. Notification of changes in risk or trigger of risk events.

The Vendor is responsible for updating the Risk Management Plan as necessary and throughout all phases of the project until the end of the contract period.

Section 30.070.050.010.060—Quality Management Plan

A formal Quality Management Plan (QMP) will be produced in order to identify quality requirements and/or standards for the project and deliverables, and to document how the project will demonstrate compliance.

PMBOK breaks down the project quality management plan into three interactive process groups:

1. Plan Quality.
2. Perform Quality Assurance
3. Perform Quality Control (QC).

Section 30.070.050.010.060.010—Plan Quality

The quality planning process applies to plans, documents, products, programs, and operational functions and will consist of:

1. Identifying which quality requirements and standards are relevant to the project and how to satisfy them.
2. Identifying and defining appropriate quality metrics and measures to establish standards for:
    a. Project processes.
    b. Product functionality.
    c. Regulatory compliance requirements.
    d. Project deliverables.
    e. Project management performance.
    f. Documentation.
    g. Testing.
3. Identifying quality standards and expectations for: customers, the project, organization, and Federal and Commonwealth mandates and initiatives including:
    a. CMS guidelines such as MITA and Medicaid and Exchange IT guidance.
4. Defining customer and project goals, quality standards, critical success factors, and metrics for which to measure success.
5. Identifying monitoring processes and the metrics to measure quality standards.
6. Defining methods of data collection and archiving, and document timeframes for measurement and metrics reporting.
7. Identifying the tools and techniques available to the analyst such as:
    a. Cost benefit analysis.
    b. Statistical sampling.
    c. Flowcharting.
    d. Benchmarking.

An outline of acceptance criteria for each phase of the project will include content checklists and establish performance measures, using tools to assess the quality of project deliverables and product delivery.

Acceptance criteria must be established well before the start of development of each planned deliverable. The DMS will review and formally approve the acceptance criteria of the deliverable.

Section 30.070.050.010.060.020—Perform Quality Assurance

Quality Assurance is a process that utilizes data from the Quality Control process that includes, but is not limited to:

1. Auditing the quality requirements and the results from the quality measurement initiatives identified in the process group.
2. Providing consistent and systematic measurement comparison with standards.
3. Monitoring processes and associated feedback loops that confer error prevention.
4. Ensuring and providing assurance to the Commonwealth that service delivery meets or exceeds the quality standard requirements.

5. Analyzing quality data, document opportunities for improvement and apply what was learned from quality analysis to eliminate gaps between current and desired levels of performance.

Quality assurance activities are usually performed by a quality assurance department or similar organization not actively involved in the work of the project. The Quality Management Plan will identify the unit singly responsible for performing the QA function for each phase of the SDLC.

In addition to the QA activities identified above, the QA unit will be responsible for:

1. Making recommendations for continuous process improvement.
2. Developing audit strategies.
3. Initiating corrective actions.
4. Organizational process asset updates, including QA policies, procedures, guidelines, and lessons learned.
5. Initiating change requests that improve performance.
6. Validating SLA performance metrics.
7. Submitting monthly status reports and findings to DMS and the Vendor.

Section 30.070.050.010.060.030—Perform Quality Control

Quality Control is performed throughout the project and employs activities and methodologies to observe and correct process variance or abnormality and ensure consistency in performance so that service quality requirements will be fulfilled. , that includes, but is not limited to:

1. Identifying those monitoring and controlling actions that will be conducted to control quality of deliverables and operational performance throughout the length of the Master Agreement.
2. Defining how it will be determined that quality standards comply with the defined standards outlined earlier in this document.
3. Identifying owners of ongoing monitoring and improvement of project processes.
4. Examining the work product to determine if it complies with the documented standard.

Quality Controls will be established for each deliverable and product by phase in a consolidated QC plan to be followed for the entire project life cycle. The QC plan will prioritize those activities that are designated as critical to FA operations and to the SLAs established by the master SLA agreement. The plan may be amended from time to time with the prior approval of DMS.

Areas in which to perform quality assurance and quality control efforts shall include, but not be limited to:

1. Project Deliverables.

2. KYMMIS implementation.
3. System component and module maintenance.
4. Change management.
5. System Documentation.
6. Testing activities.
7. Operational processing.
8. Claims processing and data entry.
9. Version control.

The Vendor is responsible for updating the Quality Management Plan as necessary and throughout all phases of the project until the end of the contract period.

Section 30.070.050.010.070—Change Management Plan

The KYMMIS Vendor should work with DMS to develop a Change Management Plan that describes the roles and responsibilities, policies, processes, and procedures necessary for controlling and managing the changes during the life of the Project. This document must identify how changes are identified, defined, evaluated, approved, and tracked through completion. This plan must identify responsibilities and define the composition, function, and procedures for a Change Management Board. Additionally, the Vendor must follow a Configuration Management Plan and version control procedures.

The Change Management Plan will identify the Vendor's proposed procedure for resolving any dispute between DMS and the KYMMIS Vendor as to whether any requirement of DMS is within the scope of work covered by the Master Agreement.

The change control process outlined in the plan must be approved by DMS and will address the process for approving system software and hardware changes as well as defect and maintenance management.

Section 30.070.050.010.080—Business Continuity Plan

The KYMMIS Vendor should deliver a preliminary Business Continuity Plan (BCP) early in the project, and continue through operations and maintenance. The BCP will be updated and tested through the operations phase as scheduled and agreed to by the Commonwealth.

The BCP will, at a minimum, identify the core business processes involved in Kentucky Medicaid, contain a risk analysis for each core business process, include an impact analysis for each core business process, and define minimum acceptable levels of outputs for each core business process. The BCP must establish adequate backup processes for all KYMMIS systems and operational functions and address the potential impacts of disaster occurrence. Contingency plans are composed of two fundamental operations: System Backup and Disaster Recovery. The BCP must be in accordance with Commonwealth standards as established by the Commonwealth.

Section 30.070.050.010.090—Disaster Recovery Plan

The KYMMIS Vendor should create and maintain a Disaster Recovery Plan (DRP) to include back-up procedures and support to accommodate the loss of online communication between the KYMMIS Vendor's processing site and Commonwealth facility(ies) in Kentucky; disasters or occurrences which cause a disruption to the processing of Kentucky transactions (claim records, eligibility verification, provider file, updates to the KYMMIS, and so forth); loss of the Vendor's primary processing site; or loss of access for the Commonwealth online component of the KYMMIS.

KYMMIS Vendor must maintain a CHFS approved BCP Plan and Disaster Recovery and System Back-up Plan at all times. It is the sole responsibility of the KYMMIS Vendor to maintain adequate backup to ensure continued automated and manual processing. The Plan must be available to CMS, CHFS, or State auditors at all times. All critical operations must be clearly defined in the KYMMIS Vendor's CHFS approved disaster recovery plan and must resume in no later than five business days following a disaster.

The KYMMIS Vendor must provide an alternate business area site in the event the primary business site becomes unsafe or inoperable.

Section 30.070.050.010.100—Training Plan

The KYMMIS Vendor should provide a Training Plan that addresses all training requirements, as directed by DMS. Information for the Training Plan is found in Learning Management System Overview Section 30.070.070.

Section 30.070.050.010.110—Testing Plan

The KYMMIS Vendor will create a testing plan that includes:

1. Unit testing.
2. System Integrated Testing (SIT).
3. User Acceptance Testing (UAT).
4. Operational Readiness Testing (ORT).
5. Parallel Testing.
6. Volume Testing.
7. Load Testing.
8. Stress Testing.

Section 30.070.050.010.110.010—Testing Overview

The KYMMIS Vendor should create and deliver to DMS a comprehensive and thorough Testing Plan. DMS will review all test results, with a special focus on structured data

tests, SIT, UATs, parallel testing, and retests of failed items. DMS will not approve the KYMMIS for implementation until all tests pass to the satisfaction of DMS. The KYMMIS Vendor shall revise and retest, as often as necessary, to meet DMS requirements.

The KYMMIS Vendor should provide all documentation for the software being tested before acceptance testing will begin. DMS will have 10 working days to review each deliverable outlined within the takeover schedule and to either notify the KYMMIS Vendor of acceptance or to provide the KYMMIS Vendor a detailed list of deficiencies that must be remedied. In the event that DMS notifies the KYMMIS Vendor of deficiencies, the KYMMIS Vendor shall correct the deficiencies within five working days, unless DMS consents in writing to a different timetable.

Upon notification by the KYMMIS Vendor that the KYMMIS has been fully implemented and is ready for final system acceptance testing, DMS will have 60 calendar days to evaluate and test the systems to confirm that they perform without any defects and perform pursuant to the specifications set forth in this RFP. The KYMMIS Vendor shall participate in the acceptance testing of the system by providing technical staff at DMS's location, to assist in demonstrating all functions of the system. DMS must sign off on each application, to ensure that it meets all functional and technical requirements. In the event that one or more applications supplied by the KYMMIS Vendor are not accepted, the KYMMIS Vendor shall correct the deficiencies or provide, at its own expense, software that may be required to meet the acceptance criteria within five calendar days or a mutually agreed upon period.

The KYMMIS Vendor shall be required to demonstrate completeness of the Takeover of the baseline system during the parallel testing task. Completeness will be measured by the completion and submission of Takeover activities, assessments, and deliverables listed in Section 30. Also, the outputs produced by the takeover KYMMIS Vendor shall be consistent with the outputs produced by the FA. Additional outputs may also be required, when enhancements are implemented.

Section 30.070.050.010.120—Hardware/Software Configuration Plan

A Hardware and Software Configuration Plan that describes the hardware infrastructure and the implementation process required to perform the Hardware/Software refresh for the KYMMIS Takeover. The current KYMMIS Vendor's Hardware/Software Configuration Plan is located on the Procurement CD.

Section 30.070.050.010.130—Configuration Management Plan

The Configuration Management Plan shall describe the administrative and technical procedures to be used throughout the project lifecycle to control system and project artifacts. The Vendor shall propose a tool for monitoring the processes to be followed for change and version control, the methods and tools to be used, and the approach to be followed. At a minimum, the plan shall describe the approach and scope. The approach includes explaining the methodology, integration, and configuration

management. The scope will describe the tasks and activities that will be performed as part of project configuration management including configuration identification, system release management, version control, audit control, and roles and responsibilities of personnel/resources.

Section 30.070.060—Project Status Reporting

Project Status Reports will be in format approved by DMS for the Takeover Project. Status meetings will be held on a schedule approved by DMS. Status Reports will be delivered no less than 24 hours before each status meeting. The Status Report will contain, at a minimum:

1. A general status report.
2. Activities completed in the preceding period.
3. Activities planned for the next period.
4. A report on issues that need to be resolved.
5. A report on the status of risks, with special emphasis on change in risks, risk triggers, or the occurrence of risk items.
6. A report on the status of each task in the WBS that is in progress or overdue.
7. A schedule variance report showing the earned value of the work completed, the planned value of the work completed, and the variance.
8. Weekly, Monthly, and Quarterly Status reports summarizing data from the agreed upon interval (e.g., weekly) reports, including financial information related to expenses and billings.
9. Executive summaries for presentation to management and oversight bodies.

Section 30.070.070—Project Staffing (See Section 60.020.010.130; 6; 125 points)

A key factor in the success of the project is the degree of collaboration between Project staff, CHFS participants, and Vendor staff. The Vendor's Project team will be responsible for performing and supporting the project with quality-related activities described throughout this Section of the SOW. CHFS expects the Vendor to staff the project team with individuals who have expertise to perform or administer the activities. Key Staff designated by the Vendor will be approved by CHFS.

In addition, the Vendor should provide qualified, highly skilled project staff. The composition of the project staff should be at the Vendor’s discretion. However, the Vendor should ensure that project staff meet and retain the performance standards defined in the Project Plan.

The CHFS Program Director works closely with the Vendor’s Project Manager on day-to-day project activities. The Vendor should have full responsibility for providing adequate staff to complete the project in the required time frame.

Section 30.070.070.010—Project Staffing Commonwealth Responsibilities

1. Create performance measures by unit and business process.
2. Create an employee calendar and schedule.
3. Define criteria for assigning activities.
4. Define the desired content, format, frequency, and media for reports.
5. Record information into the performance tracking system.
6. Analyze information from the performance tracking system.

Section 30.070.070.020—Project Staffing Vendor Requirements (Section 60.030 Section 3)

KYMMIS Vendor Staff roles will include, but are not limited to:

1. Account Manager.
2. Project Manager.
3. Quality Manager.
4. Training Coordinator.
5. Operations Manager.
6. Claims Processing Manager.
7. Systems Manager.
8. Systems Liaison Manager.
9. Web Master.
10. DSS/DW Manager.
11. DSS/DW Database Administrator (DBA).
12. Reporting Specialists.
13. Technical Writers.
14. Systems Maintenance/Modification Programmers.
15. Business Analysts (BA).
16. KYMMIS DBA.
17. Clinical Specialists.
18. DW Business Objects Universe Developer.
19. DW Data Integrator Extract, Transform, and Load (ETL) Developer.
20. DW C Programmer.

See Section 60.030 (Section 3) for staffing qualification requirements.

Section 30.070.080—Facility Overview

The KYMMIS Vendor is responsible for site preparation for its Kentucky project office. All equipment and software necessary for the Vendor to successfully takeover, design and develop, implement operate and maintain the KYMMIS will be the responsibility of the Vendor. The Vendor shall also be responsible for all hardware and software to connect to the Commonwealth of Kentucky Local Area Network (LAN) and Wide Area Network (WAN) (Commonwealth-wide area network).

DMS has a well-developed hardware and software environment infrastructure. DMS is not requesting that the KYMMIS Vendor supply workstations or printers to the user

community. The KYMMIS Vendor shall be required to supply the necessary equipment and software that will be required by the KYMMIS users beyond their standard configuration. Please refer to Sections 30.010 and 30.020 for Commonwealth Standards.

The KYMMIS Vendor shall provide access to KYMMIS tables/files via telecommunications links. All equipment and network hardware and software required to interface with Commonwealth systems must meet telecommunications and interface standards. In addition, the KYMMIS Vendor shall provide general telecommunications technical support through a help desk, for such issues as trouble shooting, device resets, passwords, and network problems. Refer to Sections 30.010 and 30.020 for Commonwealth Standards.

Section 30.070.080.010—Vendor Facility Requirements

DMS will not provide any office space or facilities to the KYMMIS Vendor. The current KYMMIS System operates in Frankfort, KY. The Commonwealth owns all software assets, the data generated by the system, and all associated documents and documentation. The KYMMIS Vendor shall identify the location where it will perform each function and service supplied by the KYMMIS Vendor. DMS requires that the KYMMIS Vendor maintain a facility within a 10-mile radius of the Cabinet for Human Resources (CHR) Building located at 275 East Main Street, Frankfort, Kentucky, 40601 throughout the term of the Contract.

The specific Vendor Responsibilities are located in Appendix L.

Section 30.070.090—IV&V Contractor Responsibilities

Independent Verification and Validation (IV&V) is a set of verification and validation activities performed to analyze system test results by an entity that is not under the control of the KYMMIS Vendor. DMS will select, through a separate procurement, an IV&V Contractor that is technically, managerially, and financially independent of the KYMMIS Vendor. The IV&V Contractor will attest that the system provided by the KYMMIS Vendor meets DMS's requirements (validation) and that the system is well engineered (verification). During the takeover and implementation phase of the project, the IV&V Contractor will work in conjunction with DMS in performing its evaluation activities.

The KYMMIS Vendor shall be working closely with DMS IV&V Contractor during all testing activities. The KYMMIS Vendor shall permit complete systems access to DMS IV&V Contractor and offer timely assistance, when requested. All project deliverables will be verified and validated by the IV&V Contractor.

Section 30.070.100—KYMMIS Operations

The KYMMIS Operations is the core of the Master Agreement and will begin immediately upon the date stated in the Master Agreement. The maintenance and operations of the KYMMIS consist of two major tasks:

1. **Operations** – Tasks necessary to monitor, correct software defects in the application systems, system enhancements, and to ensure the smooth day-to-day running of the business area processes, applications systems, and the hardware/software platform on which the applications systems reside.
2. **Medicaid Services** – Services provided to KYMMIS members, providers, and other stakeholders to enhance efficient and friendly completion of operational processes within the KYMMIS.

The various KYMMIS operations inputs, outputs, interfaces, and processes can be found in documentation, such as the MITA SS-A and KYMMIS Systems Documentation, either in the E-Procurement Directory or on the Procurement CD.

To ensure a smooth takeover, the new KYMMIS Vendor will provide all deliverables on time according to the WBS, complete testing in the allotted timeframe, and begin operating the KYMMIS as scheduled.

Section 30.070.100.010—General Operations Commonwealth Responsibilities

1. Monitor the KYMMIS Vendor's on-going quality management program.
2. Review the reporting of key performance standards and key performance indicators (KPIs).
3. Operate the Kentucky Medicaid programs.

Section 30.070.100.020—General Operations Vendor Responsibilities

Key General Operations Vendor objectives are:

1. Ensure the KYMMIS continues to meet all Federal requirements for MMIS certification and is a continually certified system, which complies with all applicable Federal and Commonwealth law, rules, and regulations.
2. Perform all of its functions according to the terms required by the State Medicaid Manual, Part 11.
3. Monitor quality and work toward continued quality improvement in for the length of the Master Agreement, in accordance with the approved Quality Management Plan (QMP).

The specific Vendor Responsibilities are located in Appendix L.

Section 30.070.100.030—Member Management Overview

The Member Management business area is a collection of business processes involved in communications between the Medicaid agency and the prospective or enrolled member and actions that the agency takes on behalf of the member. These processes share a common set of member-related data. The goal for this business area is to improve health care outcomes and raise the level of consumer satisfaction.

The maintenance of member information is required to support claim processing in batch and online mode, reporting functions, and eligibility verification. Maintenance of member-related data is also required in other functional sections, such as Third Party Liability (TPL), Long Term Care (LTC), Managed Care, EPSDT, Management and Administrative Reporting (MAR), Surveillance and Utilization Review (SUR), and Prior Authorization (PA). The current source of eligibility data for the KYMMIS is a bi-monthly file extract from the KAMES.

Section 30.070.100.030.010—Member Management Commonwealth Responsibilities

1. Determine which individuals are eligible to receive benefits, in accordance with assigned program.
2. Determine benefit limitations and applicable timeframes.
3. Determine enrollment/disenrollment information for the managed care program and any other health-management programs.
4. Maintain member information necessary to support timely and accurate claims and encounter processing and DMS initiatives.
5. Generate a file of member change transactions and provide it to the KYMMIS to be utilized for the Member Management function.
6. Assist in the correction of errors and discrepancies resulting from the member update process if the KYMMIS Vendor is unable to correct them.
7. Produce and distribute Member ID cards (currently though separate vendor).
8. Receive and respond to all member inquiries.
9. Through the eligibility (re)determination process, inform and periodically re-inform eligible members less than 21 years of age of the availability of EPSDT services and benefits, according to 42 CFR, Part 441.
10. Determine and interpret all policy and administrative decisions regarding EPSDT.
11. Through the Kentucky district offices, offer support services, as necessary, to eligible EPSDT members and arrange for those services, when requested, to aid in administering case management activities.
12. Track the provision of support services for EPSDT eligibles.
13. Perform follow-up of members who have requested services but for whom there is no indication of service provided.
14. Provide the KYMMIS Vendor with the current periodicity schedule.
15. Define the desired content, format, frequency, and media for reports.
16. Review and approve all notices for all EPSDT eligibles.
17. Monitor program effectiveness using reports produced by the KYMMIS Vendor.

18. Generate mail and track all notices for screening appointments, EPSDT services, missed appointments, the benefits of EPSDT services, periodicity schedule, dental/medical referral letter, and advance notice of loss of EPSDT eligibility.

Section 30.070.100.030.020—Member Management Vendor Responsibilities

Key Member business area objectives are:

1. Support the Automated Voice Response System (AVRS).
2. Maintain and Update Member Information.
3. Maintain and Update Buy-In Information.
4. Interface with the Commonwealth's new eligibility system.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.040—Provider Management Overview

The Provider Management business area focuses on recruiting potential providers, supporting the needs of the population, maintaining information on the provider, and communicating with the provider community. The goal of this business area is to maintain a robust provider network that meets the needs of both members and provider communities, and allows DMS to monitor and reward provider performance and improve healthcare outcomes.

The KYMMIS meets requirements of the National Provider Identifier (NPI) standards of HIPAA. This requires identifying providers by the use of a unique NPI and/or utilizes standards consistent with NPI and HIPAA requirements. The NPI number for a provider is the single identifier for a provider, identifying all locations, provider types, taxonomies, authorization, certifications, licensing for services, and other required data for that provider as a logical record.

Section 30.070.100.040.010—Provider Management Commonwealth Responsibilities

1. Develop policy governing provider participation in the KY Medicaid Program.
2. Develop format and contents of Commonwealth Provider Agreements.
3. Review and approve contents of Provider enrollment packets.
4. Provide the KYMMIS Vendor with criteria for purging providers' records.
5. Provide the KYMMIS Vendor, using file update forms or online, any changes to provider file data which come to the attention of the Commonwealth.
6. Provide all individual provider-specific payment rate updates, including mass or paper updates.
7. Approve the KYMMIS Vendor's training plan and training materials.
8. Define the desired content, format, frequency, and media for reports.

9. Provide the KYMMIS Vendor with Medicaid provider participation, enrollment, and certification information and criteria.
10. Approve, modify, print, and distribute all provider (including MCOs) issuances, billing instructions, handbooks, bulletins, and/or notices developed by the KYMMIS Vendor.
11. Monitor the accuracy of telephone information given to providers by ME Vendor staff.
12. Determine and provide the KYMMIS Vendor, in writing or by email, with any service restrictions to be placed on individual providers and to be updated to the provider data online.
13. Notify the KYMMIS Vendor of the number, sequence, and sort selection of mailing labels to be produced.
14. Review and interpret Federal Clinical Laboratory Improvement Amendments (CLIA) requirements, and inform the KYMMIS Vendor of steps that shall be taken to implement requirements through the KYMMIS.
15. Maintain interface with CLIA Online Survey, Certification, and Reporting (OSCAR) file from CMS to update provider files.
16. Enroll providers using the criteria established by the Federal government and the Commonwealth.
17. Assign provider numbers according to Commonwealth policies.
18. Maintain official, legally recognized, provider enrollment documentation.
19. Develop enrollment materials, including a provider handbook, enrollment packet, and notification letters.
20. Verify annual licensure status of Kentucky-licensed providers.

Section 30.070.100.040.020—Provider Management Vendor Responsibilities

Key Provider Management business area objectives are:

1. Maintain the NPI as the Provider ID of record.
2. Maintain a Provider Relations Call Center for providers, clients, and other inquiries.
3. Maintain a Mail Room capable of processing all outgoing and incoming and returned mail for the Commonwealth medical programs.
4. Maintain and update provider data.
5. Maintain an online provider directory.
6. Train providers.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.050—Managed Care Overview

KY Medicaid has contracted with five MCOs to coordinate health care for 85 percent of the Medicaid members. The five contracted MCOs are: 1) CoventryCares of Kentucky,

2) Kentucky Spirit Health Plan, 3) WellCare of Kentucky, 4) Humana, and 5) Passport Health Care Plan.

The MCOs are paid a monthly capitation rate applicable to each enrolled member's eligibility criteria. The Commonwealth establishes capitation rates for specific member eligibility categories based on factors, such as member program code (basis of eligibility). The MCOs are risk-bearing entities, which fund the medical care provided by their network providers from the capitation payments. Each month, each MCO is issued a payment through the KYMMIS. In addition, Brokers and Service Providers are paid a monthly capitation rate. A new ACA rule requires a medical professional be an enrolled provider in the Kentucky Medicaid Program in order to be considered for reimbursement for medical services rendered to an eligible Medicaid member.

Section 30.070.100.050.010—Managed Care Commonwealth Responsibilities

1. Perform Population and Member Outreach.
2. Manage MCO Contracts.
3. Manage Rate Setting.

Section 30.070.100.050.020—Managed Care Vendor Responsibilities

Key Managed Care business area objectives are:

1. Thoroughly test and implement interfaces with new MCOs.
2. Accept encounters from MCOs.
3. Support multiple capitation methodologies.
4. Provide data to actuarial firm chosen by the Commonwealth for calculation of capitation rates.
5. Assist the Commonwealth to coordinate data from MCO EPSDT encounters and FFS data to assemble the CMS 416 report to be submitted by the Commonwealth annually on April 1st.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.060—Operations Management Overview

The Operations Management business area is the focal point of most state Medicaid enterprises today. It includes operations that support the payment of providers, managed care organizations, other agencies, insurers, and Medicare premiums, and support the receipt of payments from other insurers, providers, and member premiums. This business area focuses on payments and receivables and "owns" all information associated with service payment and receivables. Most states have automated operations that support these payments. Common business processes include validating requests for payment and determining payable amount; responding to

premium payment schedules and determining payable amount; and identifying and pursuing recoveries.

Section 30.070.100.070—Third-Party Liability (TPL) Overview

The TPL processing function helps the Commonwealth of Kentucky utilize the private health insurance, Medicare, and other third-party resources of its medical assistance members, and ensures that Medicaid is the payer of last resort. This function works through a combination of cost avoidance (non-payment of billed amounts for which a third party may be liable) and post-payment recovery (post-payment collection of Medicaid and the Commonwealth paid amounts for which a third party is liable).

Casualty is the portion of third-party recovery that allows the Commonwealth to recover funds on claims paid for clients that are involved in personal injuries, illnesses, or other incidents in which another party may be responsible for payment. These recoveries come from potentially liable third parties and are generally pursued through litigation or filing claims with casualty insurers.

Section 30.070.100.070.010—TPL Commonwealth Responsibilities

1. Determine and direct implementation of KY Medicaid TPL policies.
2. Collect TPL information during the initial member enrollment (including managed care enrollment) and re-certification processes.
3. Collect and provide initial and ongoing third-party resource information from other available sources for all members.
4. Approve data matches and exchanges to be performed by the KYMMIS Vendor.
5. Specify, with CMS approvals, which coverage types are to be cost avoided and which are to be paid and recovered, and revise this specification when appropriate.
6. Define the desired content, format, frequency, and media for TPL reports.
7. Establish coverage type, dollar volumes, and time parameters applicable to thresholds at which accumulated claims are to be recovered or declared unrecoverable.
8. Adjust thresholds and time parameters based on the size of claim inventory.
9. Monitor estate benefit recovery.
10. Request claim facsimiles, copies of imaged claims and/or third-party billing forms as needed.
11. Identify Commonwealth users who are authorized to have access to TPL data for inquiry and/or update purposes.
12. Produce inquiry notices/letters and mail to members, providers and carriers in specified TPL situations.

Section 30.070.100.070.020—TPL Vendor Responsibilities

Key TPL business area objectives are:

1. Process data match and billing.
2. Maintain TPL Data.
3. Research Suspect Information.
4. Cost Avoidance.
5. Estate Recovery.
6. Accident Case Recovery.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.080—Claims Receipt Overview

The Claims Receipt includes Claims Control and Claims Entry. The process encompasses the receipt and processing of electronic claims, receipt and processing of encounters, and data entry and capture of paper claims and supporting attachments. A unique control number is assigned to each claim, encounter, and attachment enabling tracking from receipt to final disposition.

Claims and their supporting attachments are accepted through online entry, Optical Character Recognition (OCR)/Imaging, and electronic submission. All electronic claims and encounter submissions must be in a HIPAA compliant format.

Section 30.070.100.080.010—Claims Receipt Commonwealth Responsibilities

1. Establish image retention and retrieval standards.
2. Perform periodic review of all claim forms and provide the KYMMIS Vendor with written approval to continue receiving and entering them, to ensure these forms are the most efficient way of collecting data for claims processing.
3. Perform online entry of manual pricing of certain claims.
4. Correct/approve claims referred by the KYMMIS Vendor.
5. Review all inventory management and other operational claims reports.

Section 30.070.100.080.020—Claims Receipt Vendor Responsibilities

Key Claims Control/Claims Entry business area objectives are:

1. Provide reliable data entry of paper claims and attachments.
2. Support timely claims resolution.
3. Maintain organized and retrievable imaging of claims.
4. Provide for efficient claims processing.
5. Maintain controls and balancing procedures.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.090—Claims Adjudication/Encounters/PA Overview

The process to receive, edit, process, and pay Medicaid healthcare claims is the “heart” of the KYMMIS system. The process involves determination of submission status, information validation and editing, service coverage (Prior Authorization), TPL, healthcare coding, and pricing the claim for provider payment. The claims processing and adjudication function validates claims submitted, determines the allowed reimbursement amount, and the final disposition. Claims failing validation are suspended for correction or are denied. Claims requiring review are suspended for error resolution or manual review.

Single claim and encounter adjustments are entered online. Mass adjustments may be both entered online and system generated. All adjustments are processed through the claims processing function. Managed care encounters are also processed by the claims processing function however no payment is made for encounters.

Section 30.070.100.090.010—Claims Adjudication/Encounters/PA Commonwealth Responsibilities

1. Provide written approval of all accepted internal and external claims processing procedures that are used to adjudicate claims, and to control the audit trails and location within the claims processing system for all claims (e.g., medical policy resolution, manual pricing, etc.)
2. Monitor the KYMMIS Vendor through review of claims processing cycle balancing and control reports.
3. Define Commonwealth-approved claim forms.
4. Provide written approval of the accepted format of all electronic media claims.
5. Approve criteria and procedures for adjudication of “special” claims (e.g., bypass edit/audit conditions).
6. Provide written approval of all edits and audits.
7. Determine prepayment and medical review criteria.
8. Determine the disposition of edits and audits (i.e., suspend, claim correction form, deny report, message only).
9. Provide, on an ongoing basis, written approval of all accepted adjudication processes.
10. Provide written approval of all accepted pricing methodologies.
11. Specify error override and force policy and procedures for use by the KYMMIS Vendor in claims correction.
12. Specify those claims errors and medical review claims to be referred to the Commonwealth for correction/approval.
13. Define the desired content, format, frequency, and media for reports.
14. Review returned EOMBs and EOBs for discrepancies and produce monthly reports which identify the percentage of claims questioned, the number of claims questioned, and the dollar amount of the claims questioned.

15. Review and follow-up on reported questionable claims from returned EOMBs and EOBs.

Section 30.070.100.090.020—Claims Adjudication/Encounters/PA Vendor Responsibilities

Operational tasks include a system to balance claims, to know the location and status of every claim record, and ensure that every claim received has been properly adjudicated. All EDI and automated interface transactions are handled under a variety of connectivity methods and computer platforms.

Key Claims Processing business area objectives are:

1. Efficiently process and pay claims to providers. There will be a minimum of one payment cycle per week.
2. One hundred percent of claims will be paid, denied, or suspended during the reporting period.
3. Resolve suspended claims in a timely manner.
4. Correct and adjudicate claims with errors (error resolution).
5. Process Nursing Home and Waiver claims in the claim cycle after receipt.
6. Provide the Commonwealth with hard-copy original claim records, adjustments, and any attachments.
7. Process claims following Commonwealth policy through edits and audits.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.100—Program Management Overview

The Program Management business area houses the strategic planning, policy making, monitoring, and oversight activities. These activities depend heavily on access to timely and accurate data and the use of analytical tools. This business area uses a specific set of data (e.g., information about the benefit plans covered, services rendered, expenditures, performance outcomes, and goals and objectives) and contains business processes that have a common purpose (e.g., managing the Medicaid program to achieve the agency's goals and objectives such as by meeting budget objectives, improving customer satisfaction, and improving quality and health outcomes).

As the Medicaid enterprise matures, Program Management benefits from immediate access to information, addition of clinical records, use of standards, and interoperability with other programs. The Medicaid program is moving from a focus on daily operations (e.g., number of claims paid) to a strategic focus on how to meet the needs of the population within a prescribed budget.

Section 30.070.100.110—Financial Management Overview

The Financial Management function encompasses claim payment processing, adjustment processing, accounts receivable processing, capitation payment, capitation payment reconciliation, and all other financial transaction processing. It ensures that all funds are appropriately disbursed for claim payments and all post-payment transactions are applied accurately.

The Financial Management function is the last step in claims processing. It produces the Remittance Advices (RAs), the financial reports, and a request to the Commonwealth for check issuance or (EFT, by tape or electronic transmittal), at DMS' direction. At the end of each claims processing cycle, the Financial Management function processes each provider's finalized claims and outstanding accounts due to the Commonwealth.

Section 30.070.100.110.010—Financial Management Commonwealth Responsibilities

1. Establish financial processing, adjustment processing, and capitation payment processing policies and procedures and posting instructions.
2. Produce provider checks, based upon KYMMIS Vendor check issuance requests submitted via electronic media, and forward the checks to the KYMMIS Vendor for distribution.
3. Define expenditure summarization categories for interface with the statewide accounting system.
4. Review provider 1099 earnings reports and notify KYMMIS Vendor of any discrepancies.
5. Identify Commonwealth users who are authorized to have access to A/R data for inquiry and/or update purposes.
6. Review all other financial reports from KYMMIS Vendor.

Section 30.070.100.110.020—Financial Management Vendor Responsibilities

The KYMMIS Vendor runs the financial cycle weekly to process all financial transactions and generate payment records. These payment records are used to create electronic fund transfers (EFTs) and generate paper checks when necessary. Provider remittance advices (RAs) are created and sent to providers electronically and on paper.
Key Financial business area objectives are:

1. Maintain account ledger and financial history data.
2. Process claim adjustments.
3. Report provider earnings and 1099s.
4. Produce payments.
5. Collect Cash Receipts.

6. Produce remittance advices.
7. Follow Generally Accepted Accounting Principles (GAAP).

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.120—Reference Data Overview

Reference Data refers to the body of codes, attributes, and descriptions used by applications within or interfacing with the KYMMIS. The traditional Reference Data business area is a composite of applications that periodically update or replace tables of codes. Reference data are created and maintained by many external entities, many of which are named Standards Developing Organizations. Some of these are recognized by the U.S. Health and Human Services (HHS) as the owners or developers of data standards required by HIPAA. Reference code sets fall into very large files maintained by external entities (e.g., HCPCS, NCPDP, and ICD-9/ICD-10), small files maintained by external entities, and local code files created by the Commonwealth. Reference data maintenance includes revising code information, including HCPCS, Current Procedural Terminology (CPT), National Drug Code (NDC), and/or Revenue codes, adding rates associated with those codes, updating/adjusting existing rates, updating/adding member benefits, updating/adding provider information, adding/updating drug formulary information, and updating/adding benefit packages under which the services are available.

Section 30.070.100.120.010—Reference Data Commonwealth Responsibilities

1. Establish specific pricing criteria for all Procedure, Revenue Codes, and Drug files.
2. Identify all service codes (such as HCPCS codes), which are not covered under the FFS KY Medicaid Program.
3. Identify all service codes (such as HCPCS codes), which are covered for managed care encounters only.
4. Specify the benefit limitation and service conflict criteria to be applied through the use of the Edit/Audit Criteria file.
5. Identify all service codes (such as HCPCS, diagnosis codes) which require prior authorization.
6. Review all updates processed in response to DMS, or its designee's, requests.
7. Define the desired content format, frequency, and media for reports.
8. Respond to all inquiries from the KYMMIS Vendor regarding discrepancies in Reference File information.
9. Perform online updates, as needed.

Section 30.070.100.120.020—Reference Data Maintenance Vendor Responsibilities

Key Reference Data Maintenance business area objectives are:

1. Operate and maintain the Reference Data Maintenance function of the KYMMIS, in accordance with policy set forth by KY Medicaid.
2. Maintain current licenses for all standard codes sets within the KYMMIS at all times.
3. Maintain all Reference data and ensure that the correct information is used in claims processing.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.130—Rules Engine Overview

The Rules Engine is the core of the KYMMIS. It uses data from the Recipient Eligibility, Provider, and Reference subsystems to adjudicate claims–decide whether they should be paid and at what rate–and passes that information to the remaining subsystems for analysis, reporting, and follow up.

Section 30.070.100.130.010—Rules Engine Commonwealth Responsibilities

Provide the operational and policy parameters used by the KYMMIS Vendor to design or modify edits and audits.

Section 30.070.100.130.020—Rules Engine Vendor Responsibilities

Key Rules Engine business area objectives are:

1. Thoroughly test and troubleshoot entries and changes into the rules engine, prior to implementation, to ensure that the operation accurately parallels the existing KYMMIS.
2. Assign members to benefit plans using a rules engine.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.140—Federal Reporting Business Area Overview

The KYMMIS Vendor must provide Federal management data that produces the Management and Administrative Reporting (MAR) required for financial, benefit plan, provider, member, and funding source reporting. The KYMMIS Vendor has the responsibility of confirming that the Federal Reporting monthly summary process results are reconciled and balanced, resolving any problems associated with the outcome. The Vendor completes a monthly balancing report to ensure that Federal Reporting summarization process numbers match those generated from the weekly claim, financial, payout, and recoupment transactions, and are compared with funding source and balanced.

Section 30.070.100.140.010—Federal Reporting Commonwealth Responsibilities

1. Define required MAR reports, including the content, format, frequency, and media for the reports.
2. Initiate and/or approve in writing, all report changes, additions, or deletions, to the Management Reporting function.
3. Define Commonwealth and Federal programs, categories of service, eligibility categories, provider type and specialty codes, geographic codes, funding source codes, and other codes necessary for producing the reports.
4. Monitor production of all reports and review reports produced to assure compliance with RFP and Master Agreement requirements.
5. Review balancing reports to ensure internal and external report integrity.
6. Respond to all requests from outside sources for data on the medical assistance programs that require the use of MAR reports.
7. Provide the KYMMIS Vendor with any data required for complete financial reporting which is not generated or maintained by the systems operated by the KYMMIS Vendor.

Section 30.070.100.140.020—Federal Reporting Vendor Responsibilities

Key Federal Reporting business area objectives are:

1. Receive Extracts and Update MAR Database.
2. Produce Summary Reports.
3. Produce Expenditure Summary Reports.
4. Produce CMS Reports; EPSDT, Waiver, other.
5. Ensure all reports are produced with 100 percent accuracy and consistency in the format and type of media approved by DMS.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.140.030—Federally Required Functions

The KYMMIS Vendor must perform all functions, produce artifacts, and possess all capabilities required by CMS to maintain KYMMIS certification.

Section 30.070.100.140.040—Federally Required Data Elements

The KYMMIS must include all data elements necessary to produce required transactions, support the KYMMIS, and data elements required to maintain certification (e.g., HIPAA requires mandated transactions; therefore all data elements associated with those transactions are required and available for use within the KYMMIS).

Section 30.070.100.150—Program Management Reporting Overview

The KYMMIS Vendor must be able to generate various financial and program analysis reports to assist with budgetary controls and to ensure that the benefits and programs established are meeting the needs of the member population and are performing according to the intent of the legislative laws or Federal requirements.

Section 30.070.100.150.010—Program Management Commonwealth Responsibilities

1. Monitor production of all reports and review reports produced to assure compliance with RFP and Master Agreement requirements.
2. Review balancing reports to ensure internal and external report integrity.
3. Define Commonwealth and Federal programs, categories of service, eligibility categories, provider type and specialty codes, geographic codes, funding source codes, and other codes necessary for producing the reports.

Section 30.070.100.150.020—Program Management Vendor Responsibilities

Key Program Management business area objectives are:

1. Analyze Medicaid program costs and trends to predict impact of policy changes on programs.
2. Monitor payment processes and predict trends.
3. Analyze provider performance to show extent of participation and service delivery.
4. Analyze Member enrollment, participation, and program usage to predict utilization trends.
5. Maintain an efficient and effective management reporting process.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.160—Decision Support System (DSS)/Data Warehouse (DW) Overview

The KYMMIS must provide a DSS/DW, which will be utilized by DMS to manage data and produce reports needed for operating Medicaid and reporting to Federal requirements. A DSS is defined in the SMM Part 11 Chapter 2 Section 11276.5, B., as follows: “A DSS is often a feasible means of managing data needs. DSS is a universal term describing a menu of hardware and software components which can be combined to facilitate access to data and data analysis to serve a wide range of end-users. A DSS provides a mechanism to process data in a manageable quantity and format which is easily accessed by users to manipulate data online. A DSS can enhance the MAR and SUR functionalities by giving states the ability to access large volumes of data to

produce customized reports." The data storage and retrieval component of the DSS is often referred to as the "Data Warehouse" or the DSS relational database.

Data in the DSS/DW is refreshed periodically, on a schedule determined by CHFS. The DSS/DW supports security, data cleansing, data archiving, data management, and data standards.

Section 30.070.100.160.010—DSS/DW Commonwealth Responsibilities

1. Develop specifications for reports and data file extracts and transmit them to the KYMMIS Vendor.
2. Provide input to the KYMMIS Vendor to define parameters to be used in structuring ad hoc reporting help screens.
3. Manage the ad hoc reporting system by identifying staff who will have authority to use the ad hoc report generator software, identify and provide password restricted access to workstations from which ad hoc reports can be generated, and supervise staff persons provided by the KYMMIS Vendor.
4. Prioritize requests for ad hoc reports and data file extracts.
5. Specify downloading instructions for data extracts to be placed on the Commonwealth's LAN(s).
6. Monitor the ad hoc information retrieval function for timeliness and accuracy of outputs, and all other operational requirements specified in the contract.
   a. Complete correctly and deliver Type A Reports within 24 hours of request.
   b. Complete correctly and deliver Type B Reports within 48 hours of request.
   c. Complete correctly and deliver Type C Reports within seven days of request.
   d. Complete correctly and deliver Type D Reports within timeframe established by DMS.
   e. Complete correctly and deliver Type E Reports (Emergency reports) within two hours of request.
7. Provide other databases for use by the DSS (e.g., records from Vital Statistics, other states' Medicaid data, etc.)
8. Define data elements for use by the ad hoc and DSS.
9. Manage the DSS by identifying staff that will use the DSS and the workstations where reports can be generated.

Section 30.070.100.160.020—DSS/DW Vendor Responsibilities

Key DSS/DW business area objectives are:

1. Accept data from a variety of sources, as directed by the Commonwealth.
2. Produce data extracts timely and as specified by the Commonwealth.
3. Balance reports to validate accuracy.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.170—Program Integrity (PI) Overview

The Program Integrity (PI) business area incorporates those business activities that focus on program compliance (e.g., auditing and tracking medical necessity and appropriateness of care and quality of care, fraud and abuse, erroneous payments, and administrative abuses).

PI collects information about an individual provider or member (e.g., demographics; information about the case itself (such as case manager ID, dates, actions, and status); and information about parties associated with the case). The business processes in this business area have a common purpose (e.g., to identify case, gather information, verify information, develop case, report on findings, make referrals, and resolve case). As with the previous business areas, a single business process may cover several types of cases. The input, output, shared data, and the business rules may differ by type of case, but the business process activities remain the same.

Section 30.070.100.170.010—Program Integrity Commonwealth Responsibilities

1. Establish sample criteria and provide required inputs.
2. Request samples to be selected for reviews monthly or as needed.
3. Identify the general types of claim documentation needed to complete claim reviews and request it from the KYMMIS Vendor for sample claims.
4. Receive and review a monthly sample of Medicaid claims, hardcopy and electronic transactions, based on Commonwealth-specified sampling and stratification criteria.
5. Review output reports and supporting claim documentation and determine errors.
6. Advise the KYMMIS Vendor of detected errors.
7. Determine and monitor corrective action resulting from sample errors.
8. Determine and interpret policy and make administrative decisions relating to the sampling process.
9. Establish policy and make or delegate all administrative decisions concerning the operation of, and any changes to, the SUR reporting function.
10. Approve or request modification of the KYMMIS Vendor’s SUR reporting system training activities.
11. Approve or request modification of the SUR reporting User Manual.
12. Update the SUR management control file and determine the parameters for SUR reports.
13. Submit requests for changes to SUR report parameters to the KYMMIS Vendor at least 10 business days prior to the report cycle to which the change applies.
14. Define criteria for extraction of claim data for utilization reports.
15. Analyze all SUR reports and follow through with manual reviews and field audits, when necessary.
16. Perform detailed analysis of member and provider profiles.
17. Investigate fraud-related cases and propose corrective action.

18. Identify providers to be placed on review.
19. Monitor the KYMMIS Vendor's operation of the SUR reporting system.
20. Determine the appropriate action for questionable provider practices and member mis-utilization, and initiate an update to the provider and/or member data sets for those providers and members placed on Lock-In, prepayment review, or other restrictions.
21. Refer members to appropriate utilization programs for restriction and/or monitoring, within the constraints of current legislation.
22. Monitor restricted members and providers, and determine when to remove restrictions.
23. Submit claim detail requests and requests for provider and member profiles.

Section 30.070.100.170.020—Program Integrity Vendor Responsibilities

The Vendor will provide a Surveillance and Utilization Review (SUR) business area capability to help the Commonwealth combat Medicaid fraud, waste, and abuse. The purpose of the SUR business area is to meet the Federal requirements as found in 42 CFR Part 544 and to monitor utilization of Medicaid services to detect, investigate, and take action regarding fraud, waste, and abuse. Abuse is identified when practices are discovered which result in an unnecessary cost to the Medicaid Program, obtaining or delivering medically unnecessary services, or services that fail to meet professionally recognized standards for health care. Fraud is defined as an intentional deception or misrepresentation made by a person with knowledge that the deception could result in some unauthorized benefit to himself or some other person. Waste can include spending on services that lack evidence of producing better health outcomes compared to less-expensive alternatives; inefficiencies in the provision of health care goods and services; and costs incurred while treating avoidable medical injuries, such as preventable infections in hospitals.

The SUR Unit is concerned with the overall program integrity, and data from the SUR system can be used to investigate and track utilization and medical necessity, perform cost analysis, monitor adherence to Commonwealth policy, and look for trends and anomalies in the processing of claims.

Key SUR business area objectives are:

1. Support Commonwealth staff.
2. Train Commonwealth staff on the SUR system.
3. Research and assist Commonwealth staff with problems.
4. Update and maintain current SUR system documentation.
5. Provide a secure SUR system.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.180—Waiver Overview

The Medicaid Home and Community-Based Services (HCBS) waiver program is authorized in §1915(c) of the Social Security Act. The program permits a state to furnish an array of home and community-based services that assist Medicaid members to live in the community and avoid institutionalization. Services are provided as described in the individual's approved plan of care and may include personal care assistance, program coordination, homemaker services, respite care, and case management.

Section 30.070.100.180.010—Waiver Commonwealth Responsibilities

1. Provide KYMMIS Vendor with all documentation associated with KYMMIS waiver programs.
2. Provide KYMMIS Vendor with rules the KYMMIS Vendor is to apply into the KYMMIS system.
3. Provide the rules by which the legacy system is governed.
4. Enroll traditional and non-traditional service providers meeting identified standards of care into the program to provide services to the target population.

Section 30.070.100.180.020—Waiver Vendor Responsibilities

Key HCBS Waiver business area objectives are:

1. Process waiver provider claims and make timely and accurate payments.
2. Produce program data necessary to satisfy Federal Medicaid reporting requirements, monitor utilization, and assess quality of care provided to participants.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.190—Ancillary Components

The information contained in this section references those components that globally apply to more than one area of the KYMMIS or are supporting components to the KYMMIS.

They include:

1. Automated Letter Generation.
2. Customer Relations Management System (CRMS).
3. Document/Records/Report Management Overview.

Section 30.070.100.190.010—Automated Letter Generation

The automated letter generation function provides the capability to generate letters using standard letters or forms, letter templates, and the ability to create free-form letters. The automated letter generation function performs automated upload and

storage of letters. All letters generated through the system must be stored. The KYMMIS Vendor shall take over all letter generation functions and maintain that functionality, as designated by DMS.

The specific Vendor Responsibilities are contained in the Customer Relations Management Services section of Appendix F.

Section 30.070.100.190.020—Customer Relations Management Services (CRMS)

The CRMS includes the call center, provider service representatives, the Automated Eligibility Verification System (AEVS), letter generation, and automated call tracking system.

The Call Center shall be available 8:00 a.m. to 5:00 p.m. ET, Monday through Friday. The Call Center must answer provider and member calls an average of within 30 seconds 80% or more of the time. One hundred percent (100%) of Call Center open inquiries will be resolved and closed within five business days. Customer Service Representative accuracy must be 90 percent (90%) or higher. The Busy Out/Blocked Call rate must be less than 5 percent (5%). And the on hold rate must be less than one minute 95 percent (95%) of the time. The KYMMIS Vendor is responsible for statistics for up-to-date monitoring of the Call Center activities.

All electronic correspondence, including email, faxes, website inbox, and other electronic responses, will be responded to within two (2) business days with an interim answer and a final response within 14 calendar days. All written correspondence will be responded to within five (5) business days with an interim answer and a final response within 14 calendar days. The KYMMIS will maintain one hundred percent (100%) accuracy for all provider correspondence (electronic and written).

The EVS and AVR, and any other application providing member and provider information support must be available 24x7x365, except for scheduled and agreed upon down time. Items included in this requirement:

1. Provide a backup system to assure that downtime is limited to no more than 30 continuous minutes.
2. Provide sufficient in-bound access lines for the EVS so that providers do not encounter busy conditions at least 95% of the time.
3. Initial response must be within 4 seconds 95% of the time for AVR voice responses and electronic EVS screen responses.
4. Commercial eligibility vendors will have 99% of their transactions responded to without a time-out. CHFS must approve all commercial eligibility vendors, telecommunication carriers, and the contract between the carriers/vendors and the KYMMIS Vendor.
5. The KYMMIS Vendor shall produce a weekly report that lists average number of rings prior to calls being answered, the number and percent of calls that time out,

the number and percentage of calls that receive busy signals, the number of blocked calls, and the times and total hours of non-availability and average response times for the EVS system.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.190.030—Document/Records/Report Management Overview

The documents, records, and reports management function must be used to image all paper forms, reports, and documents received from providers, members, and other external entities that provide information or correspondence used in the business processes that make up the KYMMIS. All imaged documents must be stored and accessible from the user's desktop.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.200—Web Services Overview

The KYMMIS Vendor shall maintain the KYMMIS web portal for use by CHFS staff, providers, and other CHFS authorized parties. The web portal must have a public access area and a secure access area.

The KYMMIS Vendor shall maintain the translator functional capability, or Enterprise Application Integration (EAI) software, and EDI mapping utility capability that can process all EDI and automated interface transactions, regardless of connectivity method and computer platform.

Section 30.070.100.200.010—Web Services Commonwealth Responsibilities

1. Provide the Commonwealth EDI policies and procedures to the KYMMIS Vendor.
2. Provide web portal specifications, policies, and procedures to KYMMIS Vendor.
3. Approve content placed on web portal.

Section 30.070.100.200.020—Web Services Vendor Responsibilities

Key Web Services business area objectives are:

1. Maintain the most current and up-to-date provider manuals on the KMA website in downloadable format.
2. Maintain the EVS system on the Kentucky Medicaid website.
3. Maintain Preferred Drug List (PDL) on Kentucky Medicaid website.

4. Produce Drug Rebate invoices.
5. Maintain online PA creation, inquiry, and update.
6. Maintain the Kentucky Medical Assistance website using KEUPS as the single sign-on authentication, so that member/provider may seamlessly access relevant information stored in other state enterprise systems.
7. The Kentucky Medical Assistance website and other ancillary system components as required by CHFS, must be available 24x7x365 except for CHFS approved time for system maintenance.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.100.210—Workflow Overview

The purpose of a Workflow Management system is to document and maintain definition and modeling of workflow processes and their constituent activities in a Workflow Management Module. Workflow Management can be manual, semi-automated, or automated.

Section 30.070.100.210.010—Workflow Commonwealth Responsibilities

1. Determine policy and processes for workflow between the KYMMIS Vendor and DMS.
2. Work with the KYMMIS Vendor to facilitate efficiencies within the Workflow Management process.

Section 30.070.100.210.020—Workflow Vendor Responsibilities

Key Workflow business area Vendor objectives are:

1. Support and assist the CHFS in mapping all business processes and sub-processes to the workflow application, and in transitioning from manual to automated process execution.
2. Assist the CHFS with configuring reporting components to monitor operational activities.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.110—Security and Privacy Overview

The objective of the Security and Privacy business area is to create a Security Plan and a User Access Security Plan, that incorporate Commonwealth and Federal regulation and publications along with the functional and non-functional requirements created for the KYMMIS.

Section 30.070.110.010—Security and Privacy Vendor Deliverables

1. Security Plan.
2. User Access Security Plan.
3. Privacy Policy page.
4. Protocols for data confidentiality.

Section 30.070.110.010.010—Security Plan

The activities associated with the Security Plan include processing, capture, storage, transformation, and dissemination of information along with specifications for access for all roles and their related security level. Written approvals from the Commonwealth validate the accuracy and completeness of the documents.

Through the Security Plan, the KYMMIS Vendor describes its approach to security design and processes maintain Vendor facilities, systems, and processes to safeguard information for which the Vendor is liable. The Plan must conform to the following Commonwealth and Federal regulations and publications related to system security requirements and password usage:

1. 45 CFR Part 95.621(f) ADP System Security Requirements and Review Process.
2. Standards defined in Federal Information Processing Standards (FIPS) Publications 31, 41, and 73, issued by the National Institute of Standards and Technology (NIST).
3. National Institute of Standards and Technology (NIST) Special Publication 800-111 Storage Encryption Technologies for End User Devices.
4. National Institute of Standards and Technology (NIST) Cryptographic Module Validation List (http://csrc.nist.gov/groups/STM/cmvp/validation.html).
5. FIPS PUB 112 Password Usage, Procedure.
6. FIPS PUB 186-3 Digital Signature Standard June 2009.
7. Records Usage, Duplication, Retention, Re-disclosure and Timely Destruction Procedures/Restrictions 5 U.S.C. 552a (o) (1) (F), (H) and (I).
8. IRS Pub 1075.
9. Federal Records Retention Schedule 44 U.S.C. 3303a.
10. Privacy Act of 1974 at 5 U.S.C. 552a.
11. Computer Matching and Privacy Protection Act of 1988 (CMPPA).
12. Federal Information Security Management (FISMA).
13. SSA Information System Security Guidelines for Federal, Commonwealth, and Local Agencies.
14. Child Online Privacy Protection Act.
15. HIPAA (talk about privacy and security rules).
16. Title XIX Confidentiality Rules.

17. OASIS Web Services Security Specification 1.1.

This task shall also result in a description of the Vendor's approach to ensure the security of the KYMMIS and the data throughout the project lifecycle until contract end date. At a minimum, the outcomes of this task shall include information on:

1. Accountability, which includes the approach to establishing and maintaining security responsibility and accountability.
2. Granting or restricting access to all the applications (including Web-enabled applications) and data; auditing security events, auditing security configurations, and changes, generating security reports, and monitoring the system for vulnerabilities and intrusions.
3. Managing authorized users for user creation, assignment of new User ID (User Identification)/password/personal identification numbers (PINs), role assignments, and activity monitoring.
4. Compliance including the approach to maintaining compliance with law, standards, and best practices.
5. Technical security shall include, at a minimum, the approach to each of the following:
   a. Network segmentation.
   b. Perimeter security.
   c. Application security and data sensitivity classification.
   d. Protected Health Information (PHI) and Personally Identifiable Information (PII) data elements.
   e. Intrusion management.
   f. Monitoring and reporting.
   g. Host hardening.
   h. Remote access.
   i. 128bit encryption.
   j. Commonwealth-wide active directory services for authentication.
   k. Interface security.
   l. Security test procedures.
   m. Managing network security devices.
   n. Security patch management.
   o. Defending against viruses and mobile code.
   p. Secure Sockets Layer (SSL) for providing communications security over the Internet.

Section 30.070.110.010.010.010—Security Plan Commonwealth Responsibilities

1. Make available the appropriate personnel to participate in the Security Plan sessions.

2. Provide input and clarifications to the Vendor as needed.
3. Review and approve the Security Plan.

Section 30.070.110.010.010.020—Security Plan Vendor Responsibilities

1. Develop a Security Plan that ensures all systems, procedures, and practices are fully secured and protected.
2. Review relevant Commonwealth and Federal regulations and publications.
3. Document how Commonwealth policies, procedures will be honored with the solution.
4. Perform compliance testing.

Section 30.070.110.010.020—User Access Security Plan

The Vendor defines the approach to user access security during this task in the User Access Security Plan. At a minimum, the outcomes of this task must include a description of the following:

1. Types and relationships between the security elements, e.g., users, groups, and roles.
2. Categorization of access into different security levels that will be defined by the Commonwealth to include, at a minimum, users, groups, and roles.
3. Matrix of roles and privileges.
4. Screen/Window level security.
5. Level of authorization/security for specific functions by individual user including module level security for grouping of screens/pages.
6. Field level security including links that route to interfaces.
7. Restrictions on modifying or overriding system edits and audits or altering system functionality.
8. Types of online security checks, including security by individual, Commonwealth defined role, location, files, and fields before allowing access to any files including data, software, code, resources, or any other files resident with or accessed by the Commonwealth.
9. Types of Privacy Policy statements such as:
    a. Privacy Policy for External users, e.g., Providers.
    b. Privacy Policy for Internal users, e.g., Commonwealth.
10. Types of events that require logging in response to specific situations such as:
    a. Start up and shut down of audit functions.
    b. Successful and unsuccessful logons and logoffs.
    c. Successful and unsuccessful attempts to access security relevant files and utilities, including user authentication information.
    d. Log information on read, modify, or destroy operations.

e. Configuration changes made during auditing operations.
f. Unsuccessful usage of user identification or authentication mechanisms.
g. Changes to the time.
h. Activities that modify, bypass, or negate system security controls.
i. Use of privileged accounts.
j. Administrator logons, changes to the administrator group, and account lockouts.
k. Actions following log storage failure or exceeding threshold levels.
l. Unsuccessful security attributes revocations.
m. Modifications to user groups within a role.
n. Key recovery requests and associated responses.
o. Access denials resulting from excessive numbers of logon attempts.
p. Blocking or blacklisting of user ID, terminal, or access port.
q. Detected replay attacks.
r. Rejections of new sessions based on limits to number of concurrent sessions.
s. Use of compilers.
t. System software installations.

Section 30.070.110.010.020.010—User Access Security Plan Commonwealth Responsibilities

1. Make available the appropriate personnel to participate in the User Access Security Plan sessions.
2. Provide input and clarifications to the Vendor as needed.
3. Review and approve the User Access Security Plan.
4. Monitor system activity and act on security incidents.

Section 30.070.110.010.020.020—User Access Security Plan Vendor Responsibilities

1. Conduct walkthroughs and demonstrations during the User Access Security Plan development to enhance Commonwealth understanding and to facilitate the approval process.
2. Collaborate with the Commonwealth prior to completing the plan.
3. Prepare the User Access Security Plan, meeting the requirements as defined in this RFP.

The specific Vendor Responsibilities are contained in Attachment F.

Section 30.070.120—Learning Management Overview

The KYMMIS Vendor will provide a Training Plan that addresses all training requirements, as directed by DMS. The Training Plan shall address, at minimum:

1. The training need related to the specific phase of the project.
2. Ease of access by trainees to training (i.e., Commonwealth, Vendor, Provider, etc.).
3. Proposed training site locations and schedule.
4. Use of facilitated hands-on training sessions specific to the job function and experience level of persons requesting to be trained.
5. Deployment of Computer-Based Training (CBT) modules that address specific job functions and experience level of persons requesting to be trained.
6. Methodology on use of self-paced independent online training.
7. Methodology on use of learning experience packages.
8. Methodology for proficiency testing of trainees in facilitated hands-on and CBT sessions.
9. Availability of reinforcement training.
10. Methodology for evaluation of training effectiveness.
11. Proposed format of any training materials.
12. Process for maintaining or updating training materials based upon feedback (i.e., Commonwealth or DMS training materials review feedback, approved KYMMIS changes, DMS business rule change, etc.).
13. Process for submitting training schedule materials to the Commonwealth for review and approval prior to delivery of the training session/workshop.

The KYMMIS Vendor should, submit the final training materials to the Commonwealth for review and approval, all training material shall include:

1. Course Name, Description, Objective.
2. Instructor/Trainer guides.
3. Complete learning experience package and medium (i.e., self-paced online training, CBT module(s), trainee manual/workbook and presentation, etc.).
4. Proficiency testing tools.
5. Course/Trainer Evaluation tools.

Section 30.070.120.010—Learning Management Commonwealth Responsibilities

1. Provide the KYMMIS Vendor a copy of each attendee's written evaluation for each training session/workshop.
2. Approve, in writing, locations of training sites.
3. Provide, as the KYMMIS Vendor finalizes the training plans in support of each of the KYMMIS project tasks, a final list of other agencies and Vendors that shall be trained for each phase of the project.
4. Provide training staff responsible for monitoring all aspects of the KYMMIS Vendor's training program.

Section 30.070.120.020—Learning Management Vendor Responsibilities

Key Learning Management business area objectives are:

1. Follow approved Training Plans and provide training to DMS, KYMMIS Vendor, other Commonwealth agencies, contractors, as directed by DMS.
2. Provide training plans and training materials to the Commonwealth for review and approval, prior to delivery of the training session/workshop.
3. Develop and support a CBT application that can be accessed by various users as a training application, tutorial, or reinforcement training.
4. Provide training material that ensures a comprehensive initial and ongoing training program to all Commonwealth and non-Commonwealth staff identified by DMS, Vendor staff, and providers.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.130—Change Management Overview

The processes, procedures and system for tracking defects, routine maintenance, and modifications, or enhancements to the KYMMIS are called Change Management. The KYMMIS Vendor must provide a system and process for change management including tracking defects, maintenance matters, modifications, enhancements.

Section 30.070.130.010—Change Management Commonwealth Responsibilities

1. Participate in weekly and monthly status meetings, as defined in the Communication Plan.
2. Participate in system maintenance/defect and modification/enhancement processes.
3. Prioritize all work requests.
4. For major work requests, assist the KYMMIS Vendor in the design activities requiring project plan development (e.g., PMP, WBS, GSD, RSD, IRD, DSD).
5. Review and approve all documentation generated and/or updated.
6. Review and approve the GSD, RSD, IRD, and the DSD changes, when required.
7. Provide signoff at all levels to ensure project compliance.
8. Determine the scheduling and priorities of UAT.

Section 30.070.130.020—Change Management Vendor Responsibilities

Key Change Management Vendor Responsibilities are:

1. Provide separate processes and resources for maintenance/defect and modification/enhancement change requests.
2. Ensure changes do not alter the integrity of data across the KYMMIS.
3. Participate in weekly and monthly status meetings.

4. Produce Change Management Reports.

The specific Vendor Responsibilities are contained in Appendix L.

Section 30.070.140—Takeover Testing

Section 30.070.140.010—Operational Readiness Overview

As part of the KYMMIS Takeover Project, an Operational Readiness Test Plan (ORTP) is required for the takeover of the FA operations. The operational readiness test is designed to ensure that the KYMMIS Vendor and DMS staff are ready to process all inputs, correctly generate outputs, meet all reporting requirements, utilize a properly functioning data communications network, and have a demonstrated backup capacity. The KYMMIS Vendor shall assess the operational readiness of DMS staff that performs all business functions and operations. Operational readiness testing shall include demonstrations, load testing and results, staff readiness testing, and communications testing.

Operational readiness testing shall include all operational functions, as well as a volume and load test of several days of production capacity claim record volumes, to demonstrate the KYMMIS and the KYMMIS Vendor's staff is prepared for full production.

Operational readiness testing may include a test of actual claims processing in a full operational environment, starting with the submission of Electronic Data Interchange (EDI) transactions into the translator through the payment process, including, but not limited to, document imaging, check request, and remittance advice processing.

Testing of all other operational functions will include, but not be limited to, enrollment and eligibility processes, such as notices, member demographic changes, and capitation processing. The addition, deletion, and updating of enrollment records testing shall include, but not be limited to, a member change of address and the addition of a new member. Also, a volume test of several days of production capacity eligibility files shall be processed and will include all eligibility interface file formats.

An additional component of the operational readiness test is the demonstration and verification of data security and fire/disaster prevention and recovery procedures. The length of the test will be the amount of time that is necessary to recover from the disaster and provide proof that the recovery has been successfully completed. The KYMMIS Vendor must also assess the operational readiness of FA staff in all areas of operations.

Section 30.070.140.020—Operational Readiness Test Plan

The Operational Readiness Test Plan (ORTP) must address all aspects of Operational Readiness Testing and the Vendor's planned schedule for operational readiness testing (ORT).

Section 30.070.140.030—Operational Readiness Commonwealth Responsibilities

1. Review and approve the operational readiness test results.
2. Review and approve the systems and user documentation.
3. Confirm and signoff on the Provider Service Center's operational readiness for full functionality.
4. Conduct an operational readiness review.
5. Provide access to Commonwealth facilities, personnel, documentation and other items under its control, and provide coordination with and access to third parties, including the KYMMIS Vendor, as required for the KYMMIS Vendor to perform under the contract.
6. Review all progress reports and attend all meetings and final tests.
7. Monitor KYMMIS Vendor performance, in accordance with Master Agreement requirements and performance criteria.

Section 30.070.140.040—Operational Readiness Vendor Responsibilities

The KYMMIS Vendor shall perform specific implementation and operations functions to ensure operational readiness. In preparation for operations, the KYMMIS Vendor shall perform final file conversions (if needed), recruit and train operations staff, and conduct any necessary training to providers and DMS staff and their designees. DMS will review and approve the operational readiness test and systems and user documentation. The detailed requirements for operational readiness include, but are not limited to, those listed below:

The specific Vendor Responsibilities are contained in Attachment F.

Section 30.070.140.050—Operational Readiness Vendor Deliverables

KYMMIS Vendor deliverables for operational readiness shall include, but are not limited to:

1. Operational Readiness Test Plan (ORTP).
2. Revised operating procedures.
3. Training plan.
4. Work plan.
5. Report distribution schedule.
6. Schedules for Operational Readiness Testing (ORT).
7. Updated staffing plan for operations.
8. Parallel testing results.
9. Initial operational readiness assessment and presentation to DMS.
10. Final operational readiness assessment and presentation to DMS.
11. Assumption of operations responsibilities.

12. Initial assessment of implementation success and presentation to DMS.
13. Assessment of implementation success and presentation to DMS.
14. Takeover Readiness Report.

Section 30.070.150—Takeover Completeness

Takeover by the KYMMIS Vendor shall be considered complete when the KYMMIS Vendor has fulfilled the requirement to successfully run all systems and components of the KYMMIS and executed parallel testing with successful results. The KYMMIS Vendor shall have installed the most recent versions of the KYMMIS, including, but not limited to, all batch and online programs, telecommunications, data entry software, and test files and replacements for licensed software and systems, as described throughout this Master Agreement. If any issues develop, the KYMMIS Vendor shall coordinate with DMS to resolve problems encountered during the takeover of the KYMMIS.

Section 30.070.160—Acceptance of KYMMIS Operations

The KYMMIS Vendor shall perform all implementation functions during the takeover, as detailed in this RFP. The KYMMIS Vendor shall implement a fully operational KYMMIS on a date to be approved by DMS. The KYMMIS Vendor shall receive and be responsible for processing claims received after that date.

Fully operational is defined as processing correctly all claim types, including all claims adjustments, mass adjustments, and other financial transactions; maintaining all system files; providing access to all supporting components, including all existing subsystems; producing all required reports; meeting all system requirements; and performing all other KYMMIS Vendor responsibilities specified in this Master Agreement. If DMS determines the system will not be operational on the identified date, then implementation readiness assessments will be made until such time as DMS determines that either:

1. The system is fully operational.
2. The KYMMIS Vendor shall be deemed in default.

In the unlikely event the KYMMIS Vendor is not operational on the specified date, the KYMMIS Vendor shall be responsible for making arrangements with the FA to operate the system at the KYMMIS Vendor's expense, until the KYMMIS Vendor has the system fully operational.

Section 30.070.170—System Maintenance

The KYMMIS Vendor shall be responsible for coordinating and performing "routine maintenance," modifying, updating, and enhancing the KYMMIS throughout the term of the Master Agreement. This section of the SOW describes:

1. Definitions of defect, maintenance, modification, and enhancement.
2. How future system maintenance or fixes, modifications, or enhancements to the KYMMIS will be categorized, defined, and managed.
3. How Vendor responsibilities are defined and how programming hours will be distributed.

Section 30.070.170.010—General System Maintenance

DMS defines General System Maintenance as: Activities that include changes to a policy or rate change that may occur over time and are covered by the existing contract. This is contractually referred to as the Documented Change Request (DCR) Modification.

The KYMMIS Vendor in coordination with its subcontractors, if applicable, will be responsible for ongoing module and system component maintenance of the KYMMIS. The cost for providing ongoing systems maintenance support, including machine time, man-hours, and documentation, must be included in the fixed price proposal bid for each year of operation.

DMS considers general maintenance tasks to include preventive or corrective action(s) necessary to guarantee/ensure the integrity and timeliness of data, error-free application processing, and the adherence to performance standards for both hardware and software. Examples of functions DMS considers to be general maintenance include:

1. Source Code Updates.
2. Maintenance of password IDs, applications changes, and other data security functions.
3. Report distribution changes.
4. Report media type changes.
5. Maintenance of electronic claims receipt and Remittance Advice distribution.
6. Activities necessary to provide for continuous effective and efficient operation of the system to keep it ready and fit to perform at the standard and condition for which it was approved.
7. Activities necessary to ensure that all data, files, and programs are current and errors are corrected.
8. Activities related to file growth and partitioning.
9. File maintenance activities for updates to all files.
10. Scheduled ongoing tasks to ensure system tuning, performance, response time, database stability, and processing.
11. Changes to the job scripts or system parameters concerning the frequency, number, and media of reports.
12. Updates to software, operating systems, or other system components requiring version updates, manufacturer “patches,” and other routine manufacturer updates to software.
13. Addition of new values and changes to existing system tables and conversion of prior records, as necessary.

14. The maintenance of current system documentation, user documentation, and all program libraries.
15. Providing sufficient staff to perform all customary systems general maintenance responsibilities.

Section 30.070.170.020—Defects

DMS defines defects as: Software Error Correction and Problem Resolution – The process of "fixing errors or defects that preclude full system functionality and operability as prescribed by technical and operational requirements in the RFP, the Vendor's proposal, Design Documents or succeeding executed amendments and/or approved SOWs where the work and functionality have been previously defined and covered by the existing Master Agreement."

The KYMMIS Vendor will be required to notify DMS immediately as software errors are discovered. The Vendor will be responsible for coordinating and providing "routine" maintenance of the KYMMIS at no charge to DMS and not through use of the system modification change control process. Instead, certain coding changes and system errors/defects will be logged and tracked through a "Defect Tracking Log."

The KYMMIS Vendor is responsible for resolving all errors within the following timeframes:

a. Priority 1 Errors: Within 24 hours.
b. Priority 2 Errors: Within 5 business days.
c. Priority 3 Errors: Within an agreed upon schedule between the KYMMIS Vendor and CHFS. This will be measured on a schedule defined by CHFS.

Section 30.070.170.030—Modifications

DMS defines Modifications as: Software modifications, changes, and updates that are required when program source code must be changed to implement a system functional or performance requirement beyond the system requirements. These changes are covered by a set-aside pool of programming hours to allow a number of desired changes to be made without having to modify the contract. This is contractually referred to as the Documented Change Request (DCR) Modification.

The KYMMIS Vendor shall be responsible for coordinating and performing software modifications for all modules and component parts of the KYMMIS after its implementation, as requested by DMS. Some major program initiatives may require prior-approved Advance Planning Document Updates (APDUs) when additional resources are required. DMS will be responsible for the production of all APDUs. It is DMS's expectation that most modifications, changes, and updates will be met under the terms of the Master Agreement's firmed fixed price, which contains a provision for additional programming hours for such activities.

A modification exists when program source code must be changed to meet new functional or performance requirements beyond a module or system components existing capability. Software modifications may result when DMS or the Vendor determines that an additional requirement needs to be met or that a modification to existing file structures or current processing is needed. Modification activities will be managed through a CO request process. Examples of modification tasks include:

1. Implementation of new module or system component capabilities.
2. Activities necessary to meet new or revised CMS or other Federal or Commonwealth requirements.
3. Changes to established report, screen, or tape formats, such as sort sequence, new data elements, or report items.
4. Implementation of new edits and audits not previously contemplated in the proposed solution.

Section 30.070.170.040—Enhancements to the KYMMIS

DMS defines Enhancements as: A change that is out of scope of the existing contract and must be covered by a contract modification. This is contractually referred to as a Vendor Contract Modification Item.

When it is determined that modifications or changes to existing software and hardware significantly improve functionality and performance of the KYMMIS, the Vendor in coordination with the appropriate subcontractors, if applicable, shall make such modifications or changes as directed by DMS. DMS shall at its discretion determine whether the enhancement will be performed under the terms of the Master Agreement's firmed fixed price, which contains a provision for additional programming hours or through an amendment as the funding source.

Software enhancements may also result when DMS or the Vendor determines that an additional requirement needs to be met which results in a change to existing file structures, data sets, or current processing logic that improve performance.

Section 30.070.170.050—Software Modification/Enhancement Task Activities

Modifications may be initiated by DMS or the KYMMIS Vendor. All change requests will be prioritized and approved (or denied or modified) by DMS. The various types of modification support activity must include System Development Life Cycle Stage activities, such as:

1. Define Requirements.
2. Design Approaches.
3. Develop Technical Specifications for the selected design.
4. Develop a Test Plan.
5. Perform Documentation Creation or Updates.
6. Test module modifications and rules engine.
7. Perform Systems Integration Testing.

8. Perform acceptance Test, including regression testing.
9. Obtain approval of Acceptance Test.
10. Perform Beta Testing (not required for all changes).
11. Migrate to Production environment.
12. Perform verification of successful implementation.

The KYMMIS Vendor in coordination with the appropriate subcontractors, if applicable, must respond, in writing, to requests from DMS for estimates of system modification/enhancement efforts and schedule within 10 business days of receipt, unless specified in the CO (which may reduce that time frame) or for large project planning (which may increase that time frame). The response shall consist of a preliminary assessment of the effort (number of programmer and business analyst hours) required to complete the change by SDLC stage.

The Vendor must coordinate tracking software approved by DMS to track all CO requests and all related information, e.g., priority, staff assigned, and dates associated with each stage of development.

The Vendor shall also be responsible for reporting monthly to DMS all systems changes that have been implemented in the month. The report shall also include forecasts of CO requests with anticipated implementation dates.

DMS, at its sole discretion, may or may not choose to pursue certain modification requests. When DMS chooses to pursue a modification, a formal design estimate must be prepared by the Vendor. This estimate will define the problem to be addressed, propose a solution, and specify an estimated level of effort (number of hours) and anticipated schedule required to design, code, test, and implement the change. DMS will then approve or revise the request, assign a priority to it, and establish an expected completion date. Additional services may be requested by DMS and shall be provided on a time and materials, per diem, or other mutually acceptable financial basis as negotiated by project or activity.

Section 30.070.170.060—Systems Team Staffing/Programming Hours

The Master Agreement provides for 25,000 additional modification and enhancement hours per year above the base Master Agreement to address system issues that are not inclusive under the definition of general system maintenance.

The KYMMIS Vendor will be responsible for full-time staff support comprised of professional systems engineers (programmer/analysts) for all system maintenance change categories. This staff will be in addition to staff performing general system maintenance activities. The Vendor must identify system modification and enhancement staff to be assigned to modification and enhancement projects. Additionally, the staff can be assigned to support general maintenance activities with the approval of DMS.

The KYMMIS Vendor will provide a monthly report of time spent by job category and position. At the end of each Commonwealth fiscal year the Vendor will provide an accounting of the hours spent by job category and position during that fiscal year. If

there are any unused hours at the end of the year they will be rolled over to the next year. Hours used in excess of the 25,000 hour annual allocation may be credited to any successive year's unused balance or funded through execution of a Master Agreement amendment. At the end of the Master Agreement the Vendor and DMS will review the total hours spent versus the minimum commitments. If the Vendor fails to meet the minimum hours the Vendor will refund the balance of hours to DMS.

Qualified staff must be available to support system CO requests authorized by DMS. It is DMS's expectation that all SLAs associated with routine maintenance, software modifications, and change and enhancement requests will be met and that the work will be accomplished within the budgeted effort. In addition, it is DMS's expectation that all 25,000 programming hours will be expended in each contract year.

Section 30.070.180—System and User Documentation

The KYMMIS Vendor shall develop, prepare, print, maintain, produce, and distribute KYMMIS documentation, KYMMIS user manuals, and DMS provider manuals. DMS will develop the policy and regulations section of DMS's provider manuals. The KYMMIS Vendor is responsible for drafting provider specific billing instructions, as well as general billing instructions that are used by all provider types for the provider manuals and the eligibility verification system.

KYMMIS user manuals and DMS provider manuals will be prepared in draft form during the development/testing phase and in final form during the UAT. Operation updates to KYMMIS documentation, KYMMIS user manuals, and DMS provider manuals must be performed by the KYMMIS Vendor. The KYMMIS Vendor is responsible for preparing and printing all revisions, in final form, for all changes, corrections, or enhancements to the system and/or Medicaid program, prior to DMS sign off on the system change. Distribution of KYMMIS user manuals will be to designated DMS staff. Distribution of DMS provider manuals will be to all providers, Commonwealth staff, and any agency, organization, and/or person specified by DMS. All manuals must be available in electronic format that is compatible with DMS standards.

The KYMMIS Vendor is responsible for developing and providing to DMS complete, accurate, and timely documentation of the KYMMIS. Such documentation must be according to specifications approved by DMS. One hard copy and one electronic copy of the KYMMIS documentation must be provided within 30 calendar days following DMS acceptance of the KYMMIS during implementation. DMS acceptance will not be given and the final system documentation cannot be delivered, if portions of the ME are not functioning properly. During the operations activity, provide updated paper and electronic copies, in a format that is compatible with DMS standards, of the ME documentation within 15 calendar days following DMS acceptance of the change and prior to DMS sign off on the completion of the system change.

KYMMIS user manuals will also be provided in electronic form as a part of an online help facility, which will provide complete and up-to-date information concerning access

to all KYMMIS functions, as well as system, navigation, printing, and reporting information.

Section 30.070.190—Turnover

The KYMMIS Vendor shall be required to provide full support and assistance in turning over the complete and most current KYMMIS to the Commonwealth or its agent. Accomplishment of certain specified turnover activities by the key milestone dates, as established in the Commonwealth-approved KYMMIS Turnover Plan, shall be necessary to ensure full compliance with the start date.

Section 30.070.190—Performance Standards

The KYMMIS must meet all performance requirements and standards contained or referenced in this RFP. The KYMMIS must also be capable of producing samples, reports, and other documentation that may be required for CMS review.

Section 30.070.190.010—Performance Standards and Quality Management

The KYMMIS Vendor will implement and operate an ongoing quality management program in accordance with the project quality management plan, which includes statistical measurement and reporting of key performance standards and key performance indicators (KPIs). During the course of the contract, performance standards and KPIs will be measured and reviewed by CHFS using the Performance Monitoring System and will actively participate with the KYMMIS Vendor to approve the results, request corrective action, or assess damages as necessary.

Section 30.070.190.020—Performance Based Contracts and Damages for Vendors

Section 30.070.190.020.010—Performance Reporting

Performance standards are being implemented to improve the quality of contract performance, provide documented performance levels in critical areas of the KYMMIS's functionality, architecture, and operations, and to improve CHFS's contract management oversight and capabilities.

Section 30.070.190.020.010.010—Operations Performance Report Card

The KYMMIS Vendor in cooperation with its vendors will implement a Performance Monitoring System, at no additional cost, to provide CHFS a manual or automated method and other tools to provide reporting of the quality and performance measurements agreed upon by CHFS and the KYMMIS Vendor. The KYMMIS Vendor must document and publish desk level procedures and report results of quality analysis.

The measurements must be calculated separately from normal system processing to identify differences in quality.

Within fifteen (15) calendar days of the end of each month of operations, the KYMMIS Vendor shall be required to produce and deliver a report card on its actual performance. All Contract and performance standard requirements identified in this RFP shall be part of the report card.

The Commonwealth intends, thirty (30) days prior to each quarter, to identify twenty-five (25) performance standards of the Legacy KYMMIS Operations, Maintenance, and Modification Phases and shall use these performance standards to review the Vendor's actual performance. The Commonwealth, or its designee(s), shall reserve the right to audit records and data related to the Contractor's such performance at any time during the Contract period.

Section 30.070.190.020.010.020—Sample Operations Report Card

A sample report card is shown below. All items within each report card shall be measurable. All report cards shall be generated by the Vendor in a means that is the most efficient and accurate in order to deliver metrics to the Commonwealth as required within this RFP. Due to the changing environment of Medicaid, report cards shall be reevaluated quarterly for appropriateness and any new report cards shall be finalized through joint negotiation between the Commonwealth and the Vendor. For example, a one-time "Claims and Adjustments on Hand at Termination of Contract" report card shall be included in the last month of Contractor operations before the end of the contract period.

Table 16 – KYMMIS Report Card

MONTHLY REPORT CARD	
REPORT CARD PERFORMANCE REQUIREMENT	**Performance This Month**
SECTION 1	
The Vendor shall ensure there will be no delays or interruptions in the operation of the KY MMIS and related services caused by any failure, act, or omission of the Contractor.	MEETS
SECTION 2	
Performance Standard 1: Files: System shall be available for inquiry and update according to the terms of the contract. The Vendor shall produce a report that shows the number of hours and minutes each day the system is available.	MEETS
Performance Standard 2: Imaging: A. Select ten (10) claims weekly. Compare the date on the source document to the TCN date. Images shall be created within twenty-four (24) hours of receipt.	MEETS

MONTHLY REPORT CARD	
REPORT CARD PERFORMANCE REQUIREMENT	**Performance This Month**
Performance Standard 3: B. Sample ten (10) images a month. Record the time required to retrieve a record systematically.	MEETS
Performance Standard 4: C. Online Claims Submission: System shall be available for receipt and adjudication of claims twenty-four (24) hours per day, seven (7) days per week, except during Commonwealth-approved scheduled downtime.	MEETS
PERFORMANCE STANDARD 5:	MEETS
……	
PERFORMANCE STANDARD 25:	MEETS

Section 30.070.200—Performance Measures, Service Level Agreements, and Damages

Performance Standards:

1. The KYMMIS Vendor and its vendors will be subject to meeting performance standards with a comparison of performance against those standards made periodically at a frequency specified by CHFS. CHFS has the right to change the frequency based on Vendor performance or CHFS policy.
2. The KYMMIS Vendor and its vendors must have processes in place to monitor and self report against all performance standards.
3. In that this RFP and the resulting contract cannot contemplate every meaningful aspect current and future with the execution of the Contract, performance failures of consequence as determined by their similarity to or relatedness to other specific performance standards outlined herein and in the resulting contract shall be handled in the following manner:
   a. CHFS will notify the KYMMIS Vendor of the failure.
   b. The KYMMIS Vendor will have 10 business days to submit to CHFS a corrective action plan to address the failure.
   c. Should the corrective action plan or work plan be rejected, CHFS will assess liquidated damages of $100 per calendar day for every day a CHFS acceptable corrective action plan delivery is delayed.
   d. Upon receipt of a CHFS accepted corrective action plan, CHFS will monitor the implementation of the plan.
   e. Should the same error or performance failure reoccur the KYMMIS Vendor will be assessed liquidated damages of $1,000 for each week or part of a week in which the failure occurs up to a maximum of $52,000 per year per occurrence.

Section 30.070.200.010—Forfeiture of Retainage

In the event of the KYMMIS Vendor's failure to meet the performance standard requirements, the Vendor agrees that the Commonwealth may retain and withhold payment of a percentage of the retainage as set forth below:

1. The failure to meet one (1) performance standard requirement = forfeiture of five percent (5%) of the retainage amount;
2. The failure to meet two (2) performance standard requirements = forfeiture of ten percent (10%) of the retainage amount;
3. The failure to meet three (3) performance standard requirements = forfeiture of fifty percent (50%) of the retainage amount;
4. The failure to meet four (4) performance standard requirements = forfeiture of seventy-five percent (75%) of the retainage amount; and/or
5. The failure to meet five (5) or more performance standard requirements = forfeiture of one-hundred percent (100%) of the retainage amount.

CHFS will request corrective actions as necessary and will assess liquidated damages pursuant to the damages as specified in the Contract. Quality measurements will be reviewed by CHFS to assess any measurements that should be changed, added, or deleted for the next reporting period.

1. The KYMMIS Vendor in cooperation with its vendors will provide systems, operations, and performance monitoring tools and an automated method for monitoring the Solution's performance. All metrics used in providing reports of quality measurement required by CHFS shall be at no additional cost to the State. CHFS will have real time access to all monitoring tools, processes, and reporting.
2. The automated tools and reports will be flexible and adaptable to changes in the quality measurements required by CHFS during the Operations Phase through a rules-based engine, or component of a rules-based engine, within the Solution.
3. The Performance Monitoring System results will be posted on the public Web Site real time or as they are available to support performance measurements.
4. An independent, accredited auditing firm or qualified third party approved by CHFS may review all audit reports on a schedule defined by CHFS.

Section 30.070.200.020—Actual and Liquidated Damages

Damage may be sustained by the Commonwealth in the event that the KYMMIS Vendor fails to meet the requirements of this Contract. In the event of default or the inability to maintain minimum standards as determined by CHFS, the KYMMIS Vendor agrees to pay the Commonwealth for the actual cost of damages or the specifically outlined sums as liquidated damages as defined in this RFP. Liquidated damages are considered compensation for increased contract management cost. Liquidated damages are for those losses that CHFS cannot reasonably ascertain a specific dollar value.

Section 30.070.200.020.010—Right to Assess Damages

CHFS will assess damages based on its assessment of the KYMMIS Vendor's success in meeting required performance standards. If damages can be measured in actual cost, they are referred to as actual damages. If the damages are difficult to measure or cannot be measured in actual cost, they are referred to as liquidated damages. The KYMMIS Vendor must agree to or provide evidence acceptable to CHFS to challenge the reimbursement to the State for actual damages or the amounts set forth as liquidated damages within 30 days.

CHFS will notify the KYMMIS Vendor in writing of the proposed damage assessment. The amounts due to CHFS as actual damages may be deducted from any fees or other compensation payable to the KYMMIS Vendor or CHFS may require the KYMMIS Vendor to remit the damages within 30 days following the notice of assessment or resolution of any dispute. At CHFS's option, CHFS may obtain payment of assessed damages through one or more claims upon any irrevocable letter of credit furnished by the KYMMIS Vendor.

Section 30.070.200.020.020—Dispute Resolution Process for Damage Assessments

CHFS expects that any disputes arising under the Contract will be approached first through negotiations with the DMS staff member charged with Report Card management and second through an appeal to the Director of Information Systems or his or her designee. Legal action should only be initiated if all of these mechanisms fail.

The venue for any formal legal proceeding shall lie within the State of Kentucky. Pending final determination of any dispute, the KYMMIS Vendor shall proceed diligently with performance of the Contract and in accordance with the direction of CHFS.

Section 30.070.200.030—Consequential Damages

The KYMMIS Vendor shall, at all times, comply with all system and operational performance standard requirements and expectations specified in this RFP, with Part 11 of the State Medicaid Manual, and with all related Action Transmittals (AT) and Information Memoranda (IM), as well as any modifications or changes thereto and any changes to 42 CFR, 45 CFR, and 95 CFR as they refer to the MMIS and its operations and the use of Contractor services.

The KYMMIS Vendor further understands and agrees that it shall meet all performance standard requirements identified in the RFP during the life of this Contract. The Vendor shall, at all times, operate the KY MMIS and its activities in conformity with the policies and procedures of the Commonwealth programs.

All requirements described in the RFP shall be subject to monitoring by the Commonwealth or its designee(s). The Commonwealth reserves the right to monitor

performance and may exercise such option, at its discretion, without notice. In the event of a failure to meet the Contract or performance standards requirements, the Contractor agrees that the Commonwealth may assess and withhold from payments due its damages for the losses or the consequential damages defined in this RFP.

Section 30.070.200.030.010—Operational Start Date—Contract Requirement

The KYMMIS Vendor shall have the system fully operational on the date specified by this RFP.

If the KYMMIS Vendor does not fully meet the operational start date approved in the Finalized Work Plan, then the Vendor shall be liable for all costs incurred by the Commonwealth to continue the KYMMIS and Contractor operations. The Vendor shall also forfeit all claims for payment of monthly expenses and operational payments for that month and each month thereafter until the Commonwealth approves operational readiness.

Section 30.070.200.030.020—United States Department of Health and Human Services (US DHHS) Sanctions—Contract Requirements

The KYMMIS Vendor shall perform all of its Medicaid functions according to the terms and conditions required by the State Medicaid Manual, Part 11.

If during the KYMMIS Operations, Maintenance, and Modifications Phase, CMS imposes fiscal sanctions against the Commonwealth as a result of the KYMMIS Vendor's or any subcontractor's action or inaction, the Vendor shall compensate the Commonwealth the entire amount paid by the Commonwealth to CMS for the imposition of CMS sanctions.

Section 30.070.200.030.030—Correctness of Payments—Contract Requirements

All payments, adjustments, and other financial transactions made through the KYMMIS shall be made on behalf of eligible members to active enrolled Providers for approved services and in accordance with the payment rules and other policies of the Commonwealth.

The KYMMIS Vendor shall be liable for the actual amount of all detected erroneous payments identified as a result of Commonwealth or Federal claims reviews or as reported by Providers or from other referrals that are a result of incorrect Vendor staff action, inaccurate system data, or inaccurate processing. In addition, the Contractor shall be responsible for all costs associated with correcting the erroneous payments, including costs for re-processing, back-out processing, distribution of corrections, and so forth. Such liabilities shall be withheld from Vendor payments. The Vendor, however, may seek recovery on behalf of the Commonwealth from Providers to whom erroneous payments are made using voluntary refund, offset recovery, or other Commonwealth-approved methods.

In addition, the following requirements are included in correctness of payment:

1. The KYMMIS Vendor shall provide accurate and timely buy-in accretion and deletion based upon the Commonwealth-supplied data and the Commonwealth-approved calculation logic.
2. The KYMMIS Vendor shall provide for processing of managed care capitation payments, and management fees in the month-end claims cycle and payment in the first checkwrite of the next month.

The KYMMIS Vendor shall notify the Commonwealth immediately upon discovery of any erroneous payments, irrespective of cause, and prior to initiating appropriate recovery action. The Contractor shall use the change request process to notify the Commonwealth of any system errors that result in a potential Provider erroneous payment.

If an erroneous payment is made to a Provider and that payment is the result of a failure of the KYMMIS Vendor either to use available information or to process correctly, then the Vendor shall be liable for the erroneous payment for which full recovery cannot be made using all reasonable procedures. The Vendor shall notify the Commonwealth immediately upon discovery of any erroneous payments, irrespective of cause. The Vendor shall be responsible for any costs associated with system and operations changes associated with fixing the error(s) that caused the erroneous payment, including costs the Commonwealth or its agents incur associated with re-processing of erroneous data distributed by the Vendor.

The KYMMIS Vendor shall pay to the Commonwealth any portion of an erroneous payment not recouped within one-hundred and eighty (180) calendar days of its receipt of the direction initiating its recoupment. In addition to the amount of the erroneous payment(s), the Vendor shall be liable for interest payments at the prevailing prime beginning from the date of erroneous payment through the date of payment to the Commonwealth. The Vendor shall make such payment to the Commonwealth within seven (7) calendar days of the expiration of the one-hundred and eighty (180) calendar-day timeframe.

The Commonwealth shall not be liable to the KYMMIS Vendor for any erroneous payment due that is not recovered by recoupment from Providers. The Vendor may only initiate independent recovery procedures and actions with the prior written approval of the KYMMIS Contract Administrator once the recoupment process described herein has been completed and a repayment amount remains outstanding. The Commonwealth shall review proposed independent recovery procedures and, if reasonable, shall provide written approval. If the Commonwealth recovers any erroneous payments for which the Vendor has reimbursed the Commonwealth, the KY MMIS Contract Administrator shall notify the Vendor, who shall then submit a standard Commonwealth invoice for the returned amount, less expenses incurred by the Commonwealth during the recovery process.

Section 30.070.200.030.040—Delay or Interruption of Operations—Contract Requirement

The KYMMIS Vendor shall ensure there will be no delays or interruptions in the operation of the KY MMIS and related services caused by any failure, act, or omission of the Vendor.

Delays or interruptions in the operation of the KYMMIS and related services caused by any failure, act, or omission of the KYMMIS Vendor shall constitute a material breach. Regardless if the Commonwealth elects to terminate this Contract upon such a breach, it is nevertheless entitled to recover:

1. The difference between the cost to the Commonwealth under this Contract and the cost to it under any interim or substitute contract or other method of operation;
2. The liability of the Commonwealth to any third person arising directly or consequentially out of the Vendor's breach and cancellation of this Contract;
3. The cost to the Commonwealth of all actions taken by it to locate and secure a substitute or interim Vendor or method of operation; and
4. The loss of FFP.

In addition to the above, the Commonwealth shall reduce the KYMMIS Vendor's compensation by the following amounts:

1. Up to ten thousand dollars ($10,000.00) per calendar day, or any part thereof, for each of the first ten (10) calendar days of delay or interruption of operation continues;
2. Up to twenty thousand dollars ($20,000.00) per calendar day, or any part thereof, for each of the next twenty (20) calendar days of delay or interruption of operation continues; and
3. Up to thirty thousand dollars ($30,000.00) per calendar day, or any part thereof, for each additional calendar day of delay or interruption of operation continues after thirty (30) days.

Section 30.070.200.040—Liquidated Damages

The Commonwealth and the KYMMIS Vendor shall agree that the operation of the Legacy KYMMIS in conformity with the Contract provisions is necessary to the proper operation of DMS's programs. These programs are vital to the accurate and expeditious reimbursement of Providers of applicable medical services to eligible members and to assure continued delivery of these services to benefit-eligible members. Timely and accurate performance of this Contract shall be the essence of this Contract.

The Commonwealth and the KYMMIS Vendor shall further agree that while failures to meet certain performance standard requirements under this Contract may or will affect the delivery of medical services either directly or indirectly and may or will result directly or proximately in monetary damages to the Commonwealth, the actual amount of such injury and damage shall be impossible or extremely difficult to calculate.

Therefore, the Commonwealth and the Contractor shall agree that the Commonwealth shall reduce compensation to the KYMMIS Vendor in the instances and amounts hereinafter set forth as determined by the Commonwealth. The Parties also agree that the stated reduction in compensation amounts is reasonable and not punitive.

The KYMMIS Contract Administrator shall issue written notification to the KYMMIS Vendor of each failure to meet a performance standard requirement listed below. The imposition and reduction in compensation shall not affect any other rights of the Commonwealth to enforce or terminate this Contract.

If the Commonwealth elects not to exercise a reduction in compensation clause in a particular instance, this decision shall not be construed as a waiver of the Commonwealth's right to pursue future assessment of that performance standard requirement and associated reduction in compensation.

Section 30.070.200.040.010—Takeover Milestone Date

The KYMMIS Vendor is required to complete the Implementation of the KYMMIS by date identified in this RPF. Other deliverable key dates will be defined in the approved work plan.

If, for any reason, the KYMMIS Vendor is delayed in meeting these key dates and a Contract modification to the work plan is not approved, damages may be assessed. Approval of a Contract or work plan modification does not waive the Commonwealth's ability to impose damages if warranted by other sections of the Contract, as follows:

1. Up to $750 damages per State of Kentucky business day, or any part thereof, may be assessed for each of the first 10 calendar days of delay in meeting a key date.
2. Up to $1,500 damages per State of Kentucky business day, or any part thereof, may be assessed for each of the next 30 calendar days of delay.
3. Up to $2,500 damages per business day, or any part thereof, for each additional day of delay.

The Commonwealth retains the right to access actual damages for failure to meet key dates. The aforementioned damages in this subsection shall be in addition to any amounts assessed for delays in meeting the operational start date.

Ten thousand dollars ($10,000) may be assessed for the first month of each failure to meet any of the above requirements. Twenty thousand dollars ($20,000) may be assessed for each consecutive subsequent month a requirement remains unmet.

Section 30.070.200.040.020—Takeover Deliverable Due Dates

Copies of each deliverable, as defined in the approved Takeover KYMMIS Detailed Work Plan, shall be delivered to DMS, in final form, in the number specified and on the date specified in the approved Takeover KYMMIS Detailed Work Plan. DMS may require up to ten (10) paper copies and one (1) electronic copy of all deliverables. The electronic copy shall be compatible with Microsoft Word or other application software as requested by DMS, and submitted on the Commonwealth-specified media. All deliverables shall be in a format approved by DMS, and meet content and accuracy requirements specified or as subsequently defined by DMS.

The Commonwealth may assess one thousand dollars ($1,000.00) for each calendar day, or any part thereof, that a deliverable is late, which includes providing less than the required copies or delivery on incorrect media.

The Commonwealth may assess an additional one thousand dollars ($1,000.00) for each calendar day, or any part thereof, that a deliverable continues to not meet minimum content requirements or the approved format after its formal rejection by DMS, when appropriate.

Section 30.070.200.040.030—Takeover Key Personnel

Key personnel commitments contained in the KYMMIS Vendor's proposal for all phases of the contract shall not be changed without prior written approval of the KYMMIS Contract Administrator, unless due to the death, disability, resignation, termination, or military recall or of any named individual. Staffing includes the staff proposed for all key positions required in Section 30.070.050 within this RFP at the levels of effort proposed or as specified in the Contract.

The Commonwealth may assess up to ten thousand dollars ($10,000.00) in reduction in compensation for each key personnel proposed in the KYMMIS Vendor’s response to the RFP who is changed for reasons other than death, disability, resignation, termination, or military recall.

The Commonwealth may assess up to an additional one thousand dollars ($1,000.00) in reduction in compensation per Commonwealth business day after the initial thirty (30) Commonwealth business days allowed for KYMMIS Vendor to find an acceptable replacement for the key personnel and an acceptable replacement has not provided.

Section 30.070.200.040.040—Timeliness of Claims Processing

The KYMMIS Vendor shall meet the following requirements:

1. Adjudicate ninety-five percent (95%) of all clean claims for payment or denial within thirty (30) calendar days of receipt;
2. Adjudicate ninety-nine percent (99%) of all clean claims for payment or denial within ninety (90) calendar days of receipt;
3. Adjudicate all non-clean claims within thirty (30) calendar days of the date of correction of the condition that caused the claim to be unclean; and/or
4. Adjudicate all claims within twelve (12) months of receipt, except for those exempted from this requirement by Federal timely claims processing regulations.

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) for each failure to meet any of the requirements set forth in this Section during the first month.

The Commonwealth may reduce compensation up to twenty thousand dollars ($20,000.00) assessed for each failure to meet any of the requirements set forth in this Section within this RFP in consecutive, subsequent months.

Section 30.070.200.040.050—Failure of Notice

The KYMMIS Vendor must notify DMS in writing immediately upon discovery of any overpayments, duplicate payments, or incorrect payments regardless of cause. The KYMMIS Vendor must provide written explanation, cause, resolution, and timeframe for correction of the error per DMS requirements

The damages for failure to meet any part of the standard will equal liquidated damages of $1,000 per calendar day of delay the KYMMIS Vendor does not notify CHFS of erroneous payments

Section 30.070.200.040.060—Documentation

The KYMMIS Vendor shall be responsible for providing the Commonwealth with complete, accurate, and timely documentation of all modifications made to the operational KYMMIS. Such documentation shall be in accordance with specifications approved by DMS.

Any changes that occur to the operational system shall be documented according to specifications approved by DMS. Documentation of any such changes shall be provided to DMS.

The Commonwealth may reduce compensation up to five hundred dollars ($500.00) for each business day, or any part thereof (beginning the next business day after the documentation due date) that the required documentation has not been provided to the Commonwealth.

The Commonwealth may reduce compensation up to five hundred dollars ($500.00) for

each business day, or any part thereof, during which the documentation is unacceptable as to format, accuracy, and completeness based on DMS review. Reduction in compensation may be imposed until the Contractor provides the Commonwealth with acceptable documentation.

Section 30.070.200.040.070—Online Access to KYMMIS and Response Time

The KYMMIS Vendor shall provide the Commonwealth staff with online access to all KYMMIS online screens, systems, and data, including all Web-enabled capabilities, between the hours of 7:00 a.m. to 7:00 p.m. Eastern Time (EST or EDT as applicable) on each calendar day for ninety-nine percent (99%) of each month. The Vendor shall maintain the KYMMIS accessibility during other hours, subject to reasonable Commonwealth notification.

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) for every percentage point below ninety-nine percent (99%) for each month in which Commonwealth does not have online access available as required.

The KYMMIS Vendor must formally request CHFS approval and notify CHFS prior to any scheduled system downtime. Failure to meet the approval and notification requirements will equal $1,000 per occurrence.

The Solution's response times will be measured during normal working hours, which are 7:00 a.m. to 7:00 p.m. ET, Monday through Friday. The Website Response Times will be measured 24x7x365 except for CHFS approved time for system maintenance. Other response time requirements are as follows:

1. The Solutions Record Search Time must be within four seconds for 95% of record searches. Record Search Time is the time elapsed after the search command is entered until the list of matching records appears or loads to completion on the monitor.
2. The Solutions Record Retrieval Time must be within four seconds for 95% of records retrieved. Record Retrieval Time is the time elapsed after the retrieve command is entered until the record data appears or loads to completion on the monitor.
3. The Solutions Screen Edit Display Time must be within two seconds for 95% of the time. Screen Edit Time is the time elapsed after the last field is filled on the screen with an enter command until all field entries are edited with errors highlighted on the monitor.
4. The Solutions New Screen/Page Time must be within two seconds for 95% of the time. New Screen/Page Time is the time elapsed from the time a new screen is requested until the data from the screen appears or loads to completion on the monitor.
5. The Solutions Print Initiation Time must be within two seconds for 95% of the time. Print Initiation Time is the time elapsed from the command to print a screen or report until it appears in the appropriate queue.

6. Ad-hoc and on-demand reports within the timeframes defined by CHFS in the report request, but normally within five seconds after the request is initiated 95% of the time.
7. The Website Response Time must be within four seconds for 99% of the time. Web Site Response Time is the elapsed time from the command to view a response until the response appears or loads to completion on the monitor.
8. The EDMS (COLD) image retrieval time stored in the most recent 12 months must be within ten (10) seconds for 95% of the time. Each subsequent page of the same document (or a claim and its attachments) must be displayed in one second or less 95% of the time. Image Retrieval Time is the time elapsed after the retrieve command is entered until the image data appears or loads to completion on the monitor.

The damages for failure to meet the system response time standards in this section will equal one thousand dollars ($1,000) per hour after one hour of KYMMIS Vendor notification or one hour after any system failure, whichever occurs first.

Section 30.070.200.040.080—Claims Processing Performance Requirements

Unless otherwise indicated, the damages for failure to meet the standards listed below will equal a 2.5% reduction in the KYMMIS Vendor's monthly invoice.

Section 30.070.200.040.080.010—Online Claims Submission Availability and Response Time

The KYMMIS Vendor shall ensure online claims submission is available twenty-four (24) hours per day, seven (7) days per week, except for Commonwealth-approved maintenance timeframes. The Vendor shall provide a response for online claims submission in three (3) seconds or less ninety-nine percent (99%) of the time.

The Commonwealth shall reduce compensation by up to ten thousand dollars ($10,000.00) per hour when the online claims submission is not available for provider response for greater than one (1) hour in a calendar day, other than scheduled or Commonwealth-approved down time.

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) for every percentage point below ninety-nine percent (99%) for each month in which the response for online claims submission does not meet response time as required by Section 30.061.011.003.006.008 within this RFP.

Section 30.070.200.040.080.020—Claims Accuracy

All payments, adjustments, and other financial transactions made through the KYMMIS must be made on behalf of eligible members, to enrolled providers, for approved services, and in accordance with the Kentucky Medicaid payment rules and policies. In addition, the KYMMIS Vendor shall pay or deny claims with ninety-eight percent (98%)

accuracy as measured over a time period defined by DMS. All claims accuracy audits shall consider a random sample of five percent (5%) of the total claims processed during the applicable time period selected using a methodology previously approved by DMS. DMS may change the selection criteria targeting risk areas at DMS discretion. The KYMMIS Vendor shall be liable for the actual amount of any detected overpayments or duplicate payments identified as a result of State or Federal claims reviews or as reported by providers or from other referrals, which are a result of incorrect KYMMIS Vendor staff action or inaccurate system data and processing. Such liabilities will be withheld from KYMMIS Vendor payments. However, the KYMMIS Vendor may seek recovery, on behalf of DMS, from providers to whom erroneous payments are made, utilizing voluntary refund, offset recovery, or other State-approved methods, with approval from DMS. The KYMMIS Vendor shall notify DMS immediately upon discovery of any overpayments or duplicate payments, irrespective of cause, and prior to initiating appropriate recovery action. System errors or occurrences such as these will be logged and tracked through a Defect Tracking Log, for which the system fix which should have been previously corrected as part of the original system requirement or through the change control process. Such occurrences will be classified as a “Priority 1” error.

The consequence for failure to meet any part of the ninety-eight percent (98%) accuracy standard as measured over a time period defined by DMS will equal one thousand dollars ($1,000) per occurrence. If an overpayment or duplicate payment is made to a provider and that payment is the result of a failure of the KYMMIS Vendor to either utilize available information or to process correctly, then the KYMMIS Vendor shall be liable for the overpayment or duplicate payment for which full recovery cannot be made, using all reasonable procedures. The KYMMIS Vendor shall pay to DMS any portion of an erroneous payment not recouped within 180 calendar days of its receipt of the direction initiating its recoupment. In addition to the amount of the erroneous payment, the KYMMIS Vendor shall be liable for interest payments at the prevailing prime rate beginning from the date of erroneous payment through the date of payment to DMS. The KYMMIS Vendor shall make such payment to DMS within seven calendar days of the expiration of the 180 calendar day period. DMS shall not be liable to the KYMMIS Vendor for any erroneous payment due which is not recovered by recoupment from providers. The KYMMIS Vendor may only initiate independent recovery procedures and actions with the prior written approval of DMS once the recoupment process described herein has been completed and a repayment amount remains outstanding. If DMS recovers any erroneous payments for which the KYMMIS Vendor has reimbursed DMS, DMS shall notify the KYMMIS Vendor who shall then submit a standard State invoice for the returned amount, less expenses incurred by DMS during the recovery process.

Section 30.070.200.040.080.030—Claim Turnaround Time- Clean Claims

KYMMIS Vendor must process one hundred percent (100%) of clean claims including paper and electronic claims paid or denied within the next payment processing cycle. A clean claim means the claim is properly completed and contains all required data elements necessary for processing. The calculation for the Claim Turnaround Time

percentage will be measured on the percentage of all clean claims processed within the number of working days from the date of receipt as listed above. The performance standard does not apply with respect to a claim during the period the claim is suspended for information outside the KYMMIS Vendor's claims processing system or scope of responsibility or control.

Section 30.070.200.040.080.040—Claim Turnaround Time- Non-Clean Claims

Correct non-clean/suspended claims and adjudicate ninety-five percent (95%) within two payment processing cycles and one hundred percent (100%) within three payment cycles or 24 calendar days of the date of correction of the condition that caused the claim to be unclean.

Section 30.070.200.040.080.050—Claim Turnaround Time- All Claims

Ninety-nine percent (99%) of all claims, including paper and electronic claims, must be paid or denied within 30 calendar days of receipt unless specified differently by CHFS. The calculation for the Claim Turnaround Time percentage will be measured monthly on the percentage of all claims processed within the number of working days from the date of receipt as listed above.

Section 30.070.200.040.080.060—Adjudication of All Claims

Adjudicate all claims within 12 months of receipt, except for those exempted from this requirement by Federal timely claims processing regulations.

Section 30.070.200.040.090— Certification & HIPAA Compliance

Title 42 U.S.C. 1996 b(a)(3)(B) provides for fifty percent (50%) and seventy-five percent (75%) Federal Financial Participation (FFP) for operation of a mechanized claims payment and information retrieval system approved by CMS. Up to ninety percent (90%) enhanced FFP is available for MMIS related development costs prior approved by CMS in the State's APD and at Contract signing. The KYMMIS must, throughout the Contract period, meet all certification and re-certification requirements and maintain HIPAA compliance as established by CMS.

For any violation or loss of Federal certification, the KYMMIS Vendor will pay to the State any Federal dollar difference between the maximum allowable enhanced FFP and the amount actually received by CHFS, plus any actual damages incurred due to HIPAA non-compliance. All FFP penalty claims assessed by CMS shall be withheld from monies payable to the KYMMIS Vendor until all such damages are satisfied.

Section 30.070.200.040.090.010—HIPAA Requirements

The KYMMIS Vendor shall be required to perform the following HIPAA requirements:

1. Data mapping to identify the Protected Health Information (PHI) contained in the system and electronically transfer in order to perform HIPAA business functions.
2. A HIPAA risk analysis and develop a strategic plan to eliminate or reduce HIPAA risks. Analysis must be performed on an annual basis or at the request of CHFS at no additional cost.
3. Develop policies and procedures identifying security measures taken to protect PHI.
4. Implement audit trails to monitor PHI received; identify format, access, and purpose for use and test against policies.
5. Review Business Partner Agreements and Chain of Trust Partner Agreements with existing contracts for HIPAA compliance. Reviews will be performed on request or at least annually on a schedule determined by CHFS. The KYMMIS Vendor must provide a plan to CHFS outlining procedures for conducting reviews of contract agreements.

The Commonwealth may reduce compensation up to one thousand dollars ($1,000.00) per business day, or any part thereof, for each day the deliverable is late or unacceptable.

Section 30.070.200.040.100—Medicare Premium Payments

The State's Medicare premium liability must be paid to CMS in accordance with the U.S. Department of Health and Human Services State Buy-In Manual, publication 100-15. The KYMMIS Vendor must ensure all eligible member premiums are paid and any discrepancies with CMS are resolved on a schedule defined by CHFS.

The damages for failure to meet this standard will equal actual damages to those charges assessed by CMS in accordance with the U.S. Department of Health and Human Services State Buy-In Manual, Pub.100-15 contained in the Medicaid Procurement Library paid by the KYMMIS Vendor.

Section 30.070.200.040.110—Software Errors

The KYMMIS Vendor will be required to notify CHFS immediately as software errors are discovered. The KYMMIS Vendor shall be responsible for “routine” maintenance of the modules and system components at no charge to CHFS and not through the use of the Solution modification change control process. Instead, certain coding changes and Solution errors/defects will be logged and tracked through a “Defect Tracking Log.” CHFS will prioritize Priority 1 and Priority 2 errors.

The KYMMIS Vendor is responsible for resolving all errors within the following timeframes:

1. Priority 1 Errors: Within 24 hours.
2. Priority 2 Errors: Within 5 business days.
3. Priority 3 Errors: Within an agreed upon schedule between the KYMMIS Vendor and CHFS. This will be measured on a schedule defined by CHFS.

The damages for failure to meet the notification standard will equal one thousand dollars ($1,000.00) per calendar day from the first documented day of discovery. The damages for failure to meet the error standard will equal one thousand dollars ($1,000.00) per calendar day for each error not timely resolved.

Section 30.070.200.040.120—Change Control

The KYMMIS Vendor shall provide support for Solution modifications, changes, and updates including:

1. Statement of understanding in writing within 10 business days of receipt of Change Control (CC)
2. KYMMIS Vendor must report status of each CC timely and accurately as part of the change control process as required and requested by CHFS.
3. CCs must be completed by agreed upon date.

Updated documentation as specified by CHFS related to CC implementation including but not limited to system, user, training, or other online documentation must be provided to CHFS within 15 calendar days of CC implementation.

In accordance with the Change Management Plan described in section 30.070.030.080 of this document, the KYMMIS Vendor shall adhere to the change control process approved by CHFS for all software and hardware changes. All software and hardware releases must be planned and approved by CHFS. Release notes must be provided by the KYMMIS Vendor upon release approval by CHFS and prior to release implementation.

Damages for failure to meet any part of this standard will equal one thousand dollars ($1,000.00) per business day for each occurrence.

Section 30.070.200.040.130—Business Continuity and Contingency Plan and Disaster Recovery Plan

KYMMIS Vendor must maintain a CHFS approved BCCP Plan and Disaster Recovery and System Back-up Plan at all times. It is the sole responsibility of the KYMMIS Vendor to maintain adequate backup to ensure continued automated and manual processing. The Plan must be available to CMS, CHFS, or State auditors at all times.

Backup of all system database tables, data, and files must occur on a daily basis to preserve the integrity of both historical and current data. All current, historical, and archived data, tables, and files in the Solution and ancillary systems must be protected in an off-site location approved by CHFS to mitigate the risk of a natural or man-made disaster. The KYMMIS Vendor must supply CHFS an inventory report of all Solution database tables, data, and files backed up and archived every six months or upon CHFS request.

The KYMMIS Vendor must perform an annual disaster recovery demonstration per CHFS requirements and a review of the disaster recovery backup site, procedures for all off-site storage, and validation of security procedures. A report of disaster recovery demonstration and the backup site review must be submitted within fifteen calendar days of the review. The disaster recovery demonstration and backup site review and report submission must be concluded by June 30 each year to coincide with State fiscal year end. CHFS or the State must be able to inspect and audit the disaster recovery process at any time. CHFS or the State also reserves the right to inspect the disaster recovery backup site and procedures at any time with 24-hour notification. Any failures reported during a CHFS or State audit or the annual KYMMIS Vendor audit must be corrected based on CHFS approval and at a timeframe defined by CHFS.

The damages for failure to meet any part of the above standards will equal one thousand dollars ($1,000.00) per calendar day until the situation is resolved.

The KYMMIS Vendor must provide an alternate business area site in the event the primary business site becomes unsafe or inoperable. The KYMMIS Vendor must have backup procedures and support to accommodate the loss of online communications between the KYMMIS Vendor's processing site and the State. These procedures must specify the alternate location for the State to utilize the Solution online system and ancillary systems in the event the Solution and/or ancillary systems are down in excess of two business days.

The damages for failure to meet any part of the above standards will equal ten thousand dollars ($10,000.00) per calendar day until the situation is resolved.

Section 30.070.200.040.140—Electronic Data Processing (EDP) Audit

The KYMMIS Vendor will have completed and delivered to CHFS by June 30 of each year a report on Controls Placed in Operation and Tests of Operating Effectiveness audit performed under Statement on Standards for Attestation Engagements (SSAE) No. 16, and Assurance Reports on Controls at a Service Organization (ISAE) 3402 Reporting on Controls at a Service Organization. CHFS will specify the audit reports and level of detail for the reports delivered to CHFS each year. Audits will need to be one for both the local office and data center. The initial report coverage period shall begin at MMIS turnover and implementation and extend to the following June 30. For subsequent reports, the annual coverage period should extend from July 1 to June 30. The KYMMIS Vendor must respond with a proposed corrective action plan within 30 calendar days of receiving the audit report, if necessary. The KYMMIS Vendor must complete implementation of the State-approved corrective action plan within 40 calendar days of approval unless otherwise specified by the state. CHFS must approve the coverage period and auditor selected for the audit.

1. The damages for failure to meet the June 30 date will equal five hundred dollars ($500.00) per calendar day, or part thereof, beyond June 30 the audit is not completed to DMS satisfaction.
2. The damages for failure to meet the standard for submitting a corrective action plan will equal five hundred dollars ($500.00) per calendar day, or any part thereof, beyond the 30 calendar day requirement for submitting a corrective action plan that is satisfactory to DMS.
3. The damages for failure to meet the standard for implementing the corrective action plan will equal five hundred dollars ($500.00) per calendar day, or any part thereof, beyond the 40 calendar day requirement for implementing the corrective action plan.

Section 30.070.200.040.150—Key Turnover Phase Milestone Dates

The KYMMIS Vendor shall be required to provide full support and assistance in turning over the complete and most current KYMMIS to the Commonwealth or its agent. Accomplishment of certain specified turnover activities by the key milestone dates, as established in the Commonwealth-approved KYMMIS Turnover Plan, shall be necessary to ensure full compliance with the start date.

If, for any reason, the KYMMIS Vendor is delayed in meeting these key milestone dates and a Contract Modification to the KYMMIS Turnover Plan is not approved, a reduction in compensation may be assessed. Approval of a Contract or KYMMIS Turnover Plan modification does not waive the Commonwealth's ability to impose damages and/or reductions in compensation if warranted by other terms of the Contract.

The reductions in compensation below shall be in addition to any amounts assessed for delays in meeting the operational start date.

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) per calendar day, or any part thereof, for each of the first ten (10) calendar days of delay in meeting a milestone date.

The Commonwealth may reduce compensation up to twenty thousand dollars ($20,000.00) per calendar day, or any part thereof, each of the next twenty (20) calendar days of delay in meeting a milestone date.

The Commonwealth may reduce compensation up to thirty thousand dollars ($30,000.00) per calendar day, or any part thereof, for each additional calendar day of delay in meeting a milestone after thirty (30) days.

Section 30.070.200.040.150.010—Turnover Phase Deliverable Due Dates

Copies of each deliverable shall be delivered to DMS, when appropriate, in final form, in the number specified and on the date specified in the approved KYMMIS Turnover Plan.

DMS, when appropriate, may require up to ten (10) paper copies and one (1) electronic copy of all deliverables. The electronic copy shall be compatible with Microsoft Word or other application software as requested by DMS, when appropriate, and submitted on the Commonwealth-specified media. All deliverables shall be in a format approved by DMS, when appropriate, and meet content and accuracy requirements specified or as subsequently defined by DMS, when appropriate.

The Commonwealth may assess up to one thousand dollars ($1,000.00) for each calendar day, or any part thereof, that a deliverable is late which includes providing less than the required copies or delivery on incorrect media.

The Commonwealth may assess up to an additional one thousand dollars ($1,000.00) for each calendar day or any part thereof that a deliverable continues to not meet minimum content requirements or the approved format after its formal rejection by DMS, when appropriate.

Section 30.070.210—Compliance with other Material Contract Provisions

The objective of this standard is to provide CHFS with an administrative procedure to address general Contract compliance issues that are not specifically defined as performance requirements listed above, but are KYMMIS Vendor responsibilities contained in KYMMIS Vendor Responsibilities/Project Requirements. CHFS staff may identify Contract compliance issues resulting from deficiencies in the KYMMIS Vendor's performance through routine Contract monitoring activities. If this occurs, CHFS will notify the KYMMIS Vendor in writing of the nature of the performance issue. CHFS will also designate a period of time in which the KYMMIS Vendor must provide a written response to the notification and will recommend, when appropriate, a reasonable period of time in which the KYMMIS Vendor should remedy the non-compliance.

If the non-compliance is not corrected by the specified date, CHFS may assess liquidated damages up to the amount of two thousand dollars ($2,000.00) per State of Kentucky business day after the due date until the non-compliance is corrected.

Section 30.070.210.010—Corrective Action Plans

The KYMMIS Vendor will submit Corrective Action Plan for CHFS approval to address failures. The KYMMIS Vendor will have 10 business days to submit to DHSS a corrective action plan to address the failure.

If the Corrective Action Plan is not delivered by the specified date, CHFS may assess liquidated damages up to the amount of two thousand dollars ($2,000.00) per Kentucky business day after the due date until it is delivered.

Should the same error or performance failure reoccur the KYMMIS Vendor will be assessed liquidated damages of one thousand dollars ($1,000.00) for each week or part

of a week in which the failure occurs up to a maximum of fifty two thousand dollars ($52,000.00) per year per occurrence.

END OF SECTION 30

Section 40—Terms and Conditions

NOTE to Agency: This section is for OPS only. The Agency SHALL NOT make changes in this section, except for Section 40.030 and 40.070.

Any Vendor who has concerns regarding any terms and conditions in this RFP should submit written questions to the Commonwealth Buyer as stated in Section 10.050 of this RFP. After reviewing the questions and answers, it will become a business decision on the part of the Vendor on whether or not to proceed with the expense of preparing a response.

Proposals that take exception/deviations to Section 40 may be deemed non-responsive.

The Vendor shall not commence any billable work until a valid Contract has been executed as discussed in Section 40.010.

Section 40.010—Contract Components and Order of Precedence

The Commonwealth's acceptance of the Vendor's offer in response to the Solicitation, indicated by the issuance of a Contract Award by the Office of Procurement Services, shall create a valid Contract between the Parties consisting of the following:

1. Any written Agreement between the Parties;
2. Any Addenda to the Solicitation;
3. The Solicitation and all attachments thereto, including Section 40--Terms and Conditions of a Contract with the Commonwealth of Kentucky;
4. General Conditions contained in 200 KAR 5:021 and Office of Procurement Services' FAP110-10-00;
5. Any Best and Final Offer;
6. Any clarifications concerning the Vendor's proposal in response to the Solicitation;
7. The Vendor's proposal in response to the Solicitation.

In the event of any conflict between or among the provisions contained in the Contract, the order of precedence shall be as enumerated above.

Section 40.015—Final Agreement

The Contract represents the entire agreement between the parties with respect to the subject matter hereof. Prior negotiations, representations, or agreements, either written or oral, between the parties hereto relating to the subject matter hereof shall be of no effect upon this Contract.

Section 40.016—Agencies to Be Served

This contract shall be for use by the following agencies of the Commonwealth of Kentucky:

Cabinet for Health and Family Services (CHFS)

No shipments shall be made except upon receipt by Vendor of an official Delivery Order from a using agency.

Section 40.017—Political Subdivisions (only for All State Agency Contracts)

Under Kentucky Statutes, political subdivisions of this State including cities, counties and school districts may participate in All State Agency Master Agreements to the same extent as agencies of the Commonwealth.

Section 40.018—Extending the Contract Use to Other Agencies

The Office of Procurement Services reserves the right, with the consent of the Vendor, to offer the Master Agreement resulting from this Solicitation to other state agencies requiring the product(s) or service(s).

Section 40.019- Quantity Basis of Contract – Estimated Quantities (only for All State Agency Contracts)

Any and all quantities mentioned in this Solicitation are purely estimates, and are not to be implied nor inferred as being guarantees. The State is obligated to buy only that quantity needed by its agencies during the term of the contract. Requirements may exceed the quantities shown and the contractor will be required to furnish all requirements shown on Delivery Orders dated during the life of the contract.

Section 40.020—Contract Provisions

If any provision of this Contract (including items incorporated by reference) is declared or found to be illegal, unenforceable, or void, then both the Commonwealth and the Contractor shall be relieved of all obligations arising under such provision. If the remainder of this Contract is capable of performance, it shall not be affected by such declaration or finding and shall be fully performed.

Section 40.025—Type of Contract

The contract proposed in response to this Solicitation shall be on the basis of a **firm fixed unit price** for the elements listed in this Solicitation. This Solicitation is specifically not intended to solicit proposals for contracts on the basis of cost-plus, open-ended rate schedule, nor any non-fixed price arrangement.

Section 40.030—Term of Contract and Renewal Options

Replacement Contract

The initial term of the Replacement Contract shall be for a period of **five years** from MEMS implementation.

This Replacement Contract may be renewed at the completion of the initial Contract period for **two additional one year periods** upon the mutual agreement of the Parties. Such mutual agreement shall take the form of an addendum to the Contract under Section 40.050—Changes and Modifications to the Contract.

Takeover Contract

The initial term of the Takeover Contract shall be a period of **one year** – December 1, 2014 – November 30, 2015.

This Takeover Contract may be renewed at the completion of the initial Contract period for **two additional six month periods** upon the mutual agreement of the Parties. Such mutual agreement shall take the form of an addendum to the Contract under Section 40.050—Changes and Modifications to the Contract.

The Commonwealth reserves the right not to exercise any or all renewal options. The Commonwealth reserves the right to extend the contract for a period less than the length of the above-referenced renewal period if such an extension is determined by the Commonwealth Buyer to be in the best interest of the Commonwealth.

The Commonwealth reserves the right to renegotiate any terms and/or conditions as may be necessary to meet requirements for the extended period. The Vendor will be advised of any proposed revisions prior to the renewal periods. In the event proposed revisions cannot be agreed upon, either party shall have the right to withdraw without prejudice from either exercising the option or continuing the contract in an extended period.

Section 40.035—Basis of Price Revisions

PRICE ADJUSTMENTS: Unless otherwise specified, the prices established by the Contract resulting from this Solicitation shall remain firm for the contract period subject to the following:

A: Price Increases: A price increase shall not occur during the first twelve (12) months of the contract. A vendor may request a price increase after twelve (12) months of the contract, which may be granted or denied by the Commonwealth. Any such price increase shall be based on industry wide price changes. The Contract holder must request in writing a price increase at least thirty (30) days prior to the effective date, and shall provide firm proof that the price increase(s) is justified. The Office of Procurement

Services may request additional information or justification. If the price increase is denied, the Contract holder may withdraw from the Contract without prejudice upon written notice and approval by the Office of Procurement Services. Provided, however, that the Vendor must continue service, at the Contract prices, until a new Contract can be established (usually within sixty (60) days).

B: Price Decreases: The Contract price shall be reduced to reflect any industry wide price decreases. The Contract holder is required to furnish the Office of Procurement Services with notice of any price decreases as soon as such decreases are available.

C: Extended Contract Periods: If the Contract provides for an optional renewal period, a price adjustment may be granted at the time the Contract is renewed, subject to price increase justification as required in Paragraph A "Price Increases" as stated above.

Section 40.040—Multiyear Contracts

If this Contract is for a term that extends beyond the end of the biennium in which the Contract was made, payment and performance obligations for succeeding fiscal years are subject to the availability of funds therefor. When funds are not appropriated or otherwise made available to support continuation of performance of the Contract beyond the biennium, the Contract for such subsequent year(s) may be canceled and the Contractor shall be reimbursed in accordance with Section 40.150—Provisions for Termination of the Contract.

Section 40.045— Contract Usage (only for All State Agency Contracts)

As a result of this RFP, the contractual agreement with the selected Vendor will in no way obligate the Commonwealth of Kentucky to purchase any services or equipment under this contract. The Commonwealth agrees, in entering into any contract, to purchase only such services in such quantities as necessary to meet the actual requirements as determined by the Commonwealth.

Section 40.048—Addition or Deletion of Items or Services

The Office of Procurement Services reserves the right to add new and similar items, with the consent of the Vendor, to any contract awarded from this Solicitation. The Office of Procurement Services to effect this change will issue a Contract Modification. Until such time as the Vendor receives a Modification, the Vendor shall not accept Delivery Orders from any agency referencing such items or services.

Section 40.050—Changes and Modifications to the Contract

Pursuant to KRS 45A.210(1) and 200 KAR 5:311, no modification or change of any provision in the Contract shall be made, or construed to have been made, unless such modification is mutually agreed to in writing by the Contractor and the Commonwealth, and incorporated as a written amendment to the Contract and processed through the

Office of Procurement Services and approved by the Finance and Administration Cabinet prior to the effective date of such modification or change pursuant to KRS 45A.210(1) and 200 KAR 5:311. Memorandum of understanding, written clarification, and/or correspondence shall not be construed as amendments to the Contract.

If the Contractor finds at any time that existing conditions made modification of the Contract necessary, it shall promptly report such matters to the Commonwealth Buyer for consideration and decision.

Section 40.055—Changes in Scope

The Commonwealth may, at any time by written order, make changes within the general scope of the Contract. No changes in scope are to be conducted except at the approval of the Commonwealth through the process described in Section 40.050—Changes and Modifications to the Contract.

Section 40.060—Contract Conformance

If the Commonwealth Buyer determines that deliverables due under the Contract resulting from this Solicitation are not in conformance with the terms and conditions of the Contract and the mutually agreed-upon project plan, the Buyer may request the Contractor to deliver assurances in the form of additional Contractor resources and to demonstrate that other major schedules will not be affected. The Commonwealth shall determine the quantity and quality of such additional resources and failure to comply may constitute default by the Contractor.

Section 40.065—Assignment

The Contractor shall not assign the Contract in whole or in part or any payment arising therefrom without the prior written consent of the Commonwealth Buyer. Any purported assignment is void.

Section 40.070—Notices

After the Award of Contract, all programmatic communications with regard to day-to-day performance under the contract are to be made to the Agency technical contact(s) identified below:

Bob Nowell, Director
Division of Information Systems
Department for Medicaid Services
Cabinet for Health and Family Services
275 East Main Street
Mailstop 6 CA
Frankfort, Kentucky 40621
502-564-5183
Robert.Nowell@ky.gov

After the Award of Contract, all communications of a contractual or legal nature are to be made to the Commonwealth Buyer.

Section 40.075—Payment

The Commonwealth will make payment within thirty (30) working days of receipt of Contractor's invoice or of acceptance of goods and/or services in accordance with KRS 45.453 and KRS 45.454.

Payments are predicated upon successful completion and acceptance of the described work, services, supplies, or commodities, and delivery of the required documentation. Invoices for payment shall be submitted to the Agency Contact Person or his representative.

In the event of a failure to meet the Contract or performance standards requirements, the Contractor agrees that the Commonwealth may assess and withhold from payments due its liquidated damages for the losses defined in Section 40.075.070 within this RFP, or the consequential damages defined in Section 40.075.060 within this RFP at the Commonwealth's discretion.

Specific payment schedules can be found in the following sections:

1. MEMS Design, Development, and Implementation (DDI) Phase - Section 40.075.020
2. Takeover KYMMIS Design, Development, and Implementation (DDI) Phase - Section 40.075.025
3. MEMS Fiscal Agent Operations - Section 40.075.030
4. MEMS Software Maintenance and Modification – Section 40.075.040

Section 40.075.010 Design, Development, and Implementation (DDI) and Warranty Period Milestone payments

The Commonwealth shall require a retainage in an amount equal to ten percent (10%) of the final negotiated price for the base contract.

The documentation to be delivered during the DDI and Warranty phase and proposed payment schedule shall be concurrent with the milestone schedule located in Section 30.060.050. Payment shall not be issued for a milestone until all products associated with the Milestone have been approved in their final state by the Commonwealth. The Commonwealth shall consider a deliverable document or other product to be delivered in optimal condition if:

1. The indicators of quality and completeness contained in Appendix G – Deliverables are met.

2. The Vendor satisfactorily addresses all comments and concerns of the Commonwealth, documented in its review of the initial submission of the product, in the first re-submission.

During the warranty period, the Vendor shall deliver a monthly maintenance report which will include an application/operations performance report card as described in Section 40.075.030. The Commonwealth shall consider a monthly maintenance report to be delivered in optimal condition if:

1. The monthly maintenance report meets the quality and completeness contained in Section 40.075.020.020, and
2. The performance report card shows that all of the performance standards in Section 2 of the performance report card have been met.

Section 40.075.020—New KY MEMS Design, Development and Implementation (DDI) Phase

Payment for the DDI of the new KY MEMS activities shall be made to the Contractor as set forth below.

1. Ninety percent (90%) of the total price for the Design Activity shall be paid for:
    a. CHFS approval of the detailed Project Work Plan,
    b. CHFS approval of the RSD,
    c. CHFS approval of the GSD, and
    d. CHFS approval of the DSD.
2. Ninety percent (90%) of the total price for the Development/Testing Activity shall be paid for:
    a. CHFS approval of System Test Plan,
    b. CHFS approval of System Test Results,
    c. CHFS approval of KY MEMS User Manuals,
    d. CHFS approval of KY MEMS Operating Procedures,
    e. CHFS approval of KY MEMS Provider Manual Sections,
    f. CHFS approval of Disaster Recovery Plan,
    g. CHFS approval of the Integrated Test Facility,
    h. CHFS approval of the Integrated Test Facility Procedures, and
    i. CHFS approval of Revised Detailed System Design.
3. Ninety percent (90%) of the total price for the Conversion Activity shall be paid for:
    a. CHFS approval of Conversion Plan,
    b. CHFS approval of Conversion Test Results, and
    c. CHFS approval of all preliminary converted files.
4. Ninety percent (90%) of the total price for the User Acceptance Testing Activity shall be paid for:
    a. CHFS approval of the User Acceptance Test Resolutions Document,
    b. CHFS approval of the updated KY MEMS User Manuals,
    c. CHFS approval of the updated KY MEMS Provider Manual Sections,

    d. CHFS approval of Contractor's Operational Readiness Report; and
    e. CHFS approval of test tracking system.
5. Ninety percent (90%) of the total price for the Implementation Activity shall be paid for:
    a. CHFS approval of final file conversions,
    b. CHFS approval of final KY MEMS Systems Documentation,
    c. CHFS approval of the Implementation Plan,
    d. CHFS approval of the completion of training activities, and
    e. CHFS approval of the Contractor's notice that the KY MEMS is fully operational for all claim types.
6. Ninety percent (90%) of the total price for the Certification Activity shall be paid for:
    a. New KY MEMS certification approval from CMS.
7. Ten percent (10%) of the total price for the Design Activity; Development and Testing Activity; Conversion Activity; User Acceptance Testing Activity; Implementation Activity; and Certification Activity shall be paid for:
    a. Completion of all activities within the New KY MEMS DDI Phase and certification approval from CMS.

Payment for Option to Buy components' DDI phases will follow the same milestones listed above.

Section 40.075.025—Takeover KYMMIS Design, Development, and Implementation (DDI) Phase

Payment for the Design, Development, and Implementation of the takeover of the KY MMIS activities shall be made to the Contractor as set forth below.

1. Ninety percent (90%) of the total price for the Design Activity shall be paid for:
    a. CHFS approval of the detailed Project Work Plan.
2. Ninety percent (90%) of the total price for the Development/Testing Activity shall be paid for:
    a. CHFS approval of System Test Plan.
    b. CHFS approval of System Test Results.
    c. CHFS approval of KY MMIS User Manuals.
    d. CHFS approval of KY MMIS Operating Procedures.
    e. CHFS approval of KY MMIS Provider Manual Sections.
    f. CHFS approval of Disaster Recovery Plan.
    g. CHFS approval of the Integrated Test Plan.
    h. CHFS approval of the Integrated Test Procedures.
3. Ninety percent (90%) of the total price for the User Acceptance Testing Activity shall be paid for:
    a. CHFS approval of the User Acceptance Test Resolutions Document.
    b. CHFS approval of the updated KY MMIS User Manuals.
    c. CHFS approval of the updated KY MMIS Provider Manual Sections.
    d. CHFS approval of Contractor's Operational Readiness Report.

e. CHFS approval of test tracking system.

4. Ninety percent (90%) of the total price for the Implementation Activity shall be paid for:
    a. CHFS approval of final KY MMIS Systems Documentation.
    b. CHFS approval of the Transition Plan.
    c. CHFS approval of the completion of training activities.
    d. CHFS approval of the Contractor's notice that the KY MMIS is fully operational for all claim types.
5. Ten percent (10%) of the total price for the Design Activity; Development and Testing Activity; User Acceptance Testing Activity; and Transition Activity shall be paid for completion of all activities within the New KY MEMS DDI Phase.

Section 40.075.030—MEMS Fiscal Agent Payments (Replacement & Takeover)

For payment purposes, in each bid price year for FA operations, as bid in Pricing Schedules F and R , one-twelfth (1/12) of the firm-fixed price base cost for the bid price year shall be invoiced by the Vendor for monthly FA operations. Each monthly payment for FA operations during each bid price year shall be adjusted by (1) reduction for forfeiture of retainage as described in Section 40.075.020.040 within this RFP; (2) reduction for consequential and/or liquidated damages as described in Sections 40.075.060 and 40.075.070 within this RFP; and/or (3) credit for retainage not forfeited. The Commonwealth shall pay the invoice minus any reductions including retainage, forfeiture of retainage, and/or damages as set forth in this RFP. At the end of the last month of the bid price year, a payment adjustment will be made as follows:

1. The total number of claims actually processed during the bid price year will be determined.
2. The actual compensation due to the Contractor for that bid price year will be determined by comparing the total number of claims actually processed during the bid price year. If the actual claim volume falls anywhere within the claims volume range for the bid price year, the Contractor shall be paid that associated firm-fixed price base cost amount. Payments for claim volumes that are greater than the claims volume range for the bid price year, but less than twenty percent (20%) above the high volume of the claims volume range, shall be paid at the firm-fixed price per claim bid on Pricing Schedule D.
3. Adjustment(s) shall be made for any forfeiture of retainage and/or damages over the bid price year and any retainage amounts due the Contractor over the bid price year, as set forth in this RFP.
4. If the total amount to be paid to the Contractor over the bid price year is equal to the actual compensation due to the Contractor, no payment adjustment shall be made.
5. If the total amount to be paid to the Contractor over the bid price year is less than the actual compensation due to the Contractor, a payment adjustment of the difference shall be made to the Contractor.

6. If the total amount to be paid to the Contractor over the bid price year is more than the actual compensation due to the Contractor, a payment refund of the difference shall be immediately due from the Contractor to the Commonwealth.

Note: If, at the end of any contract year, it is determined that the actual claim volume was less than the lowest volume in the claims volume range or greater than twenty percent (20%) above the highest volume in the claims volume range for the bid price year, the Commonwealth and Contractor shall renegotiate.

Payment for Option to Buy components operations will follow the same payment arrangement listed above.

Section 40.075.030.010—Operations Performance Report Card

Within fifteen (15) calendar days of the end of each month of operations, the Contractor shall be required to produce and deliver a report card on its actual performance. All Contract and performance standard requirements identified in this RFP shall be part of the report card. There shall be two (2) sections to the report card, see example below. The first section shall address all Contract and performance standards identified in Sections 40.075.060 and 40.075.070 within this RFP and shall not be subject to forfeiture of retainage as defined in Section 40.075.020.006 within this RFP. The second section shall address any and all performance standard requirements identified in Section 30 within this RFP or offered in the Contractor's proposal that are not identified in Sections 40.075.060 and 40.075.070 within this RFP.

The Commonwealth intends, thirty (30) days prior to each quarter, to identify twenty-five (25) performance standards of the new KY MEMS Operations, Maintenance, and Modification Phases and shall use these performance standards to review the Contractor's actual performance. The Commonwealth, or its designee(s), shall reserve the right to audit records and data related to the Contractor's such performance at any time during the Contract period.

Section 40.075.030.020—Sample Operations Report Card

A sample report card is shown below. All items within each report card shall be measurable. All report cards shall be generated by the Contractor in a means that is the most efficient and accurate in order to deliver metrics to the Commonwealth as required within this RFP. Due to the changing environment of Medicaid, report cards shall be reevaluated quarterly for appropriateness and any new report cards shall be finalized through joint negotiation between the Commonwealth and the Contractor. For example, a one-time "Claims and Adjustments on Hand at Termination of Contract" report card shall be included in the last month of Contractor operations before the end of the contract period.

NOTE: THIS REPORT CARD FOR EXAMPLE PURPOSES ONLY.

Table 17 – MEMS Report Card

MONTHLY REPORT CARD	
REPORT CARD PERFORMANCE REQUIREMENT	**Performance This Month**
SECTION 1	
The Contractor shall ensure there will be no delays or interruptions in the operation of the KY MMIS and related services caused by any failure, act, or omission of the Contractor.	MEETS
SECTION 2	
Performance Standard 1: Files: System shall be available for inquiry and update according to the terms of the contract. The Contractor shall produce a report that shows the number of hours and minutes each day the system is available.	MEETS
Performance Standard 2: Imaging: A. Select ten (10) claims weekly. Compare the date on the source document to the TCN date. Images shall be created within twenty-four (24) hours of receipt.	MEETS
Performance Standard 3: B. Sample ten (10) images a month. Record the time required to retrieve a record systematically.	MEETS
Performance Standard 4: C. Electronic Claims Submission: System shall be available for receipt and adjudication of claims twenty-four (24) hours per day, seven (7) days per week, except during Commonwealth-approved scheduled downtime.	MEETS
PERFORMANCE STANDARD 5:	MEETS
……	
PERFORMANCE STANDARD 25:	MEETS

Section 40.075.030.030—Forfeiture of Retainage

In the event of the Contractor's failure to meet the ongoing operational performance standard requirements, the Contractor agrees that the Commonwealth may retain and withhold payment of a percentage of the retainage as set forth below:

1. The failure to meet one (1) performance standard requirement = forfeiture of five percent (5%) of the retainage amount.
2. The failure to meet two (2) performance standard requirements = forfeiture of ten percent (10%) of the retainage amount.
3. The failure to meet three (3) performance standard requirements = forfeiture of fifty percent (50%) of the retainage amount.
4. The failure to meet four (4) performance standard requirements = forfeiture of seventy-five percent (75%) of the retainage amount.
5. The failure to meet five (5) or more performance standard requirements = forfeiture of one hundred percent (100%) of the retainage amount.

Section 40.075.040—Software Maintenance and Modifications Payments

For payment purposes, in each bid price year for software maintenance, and modifications, as bid in Pricing Schedules E, one-twelfth (1/12) of the firm-fixed price base cost for the bid price year shall be invoiced by the Vendor for monthly maintenance, and modifications. Each monthly payment for maintenance, and modifications during each bid price year shall be adjusted by (1) reduction for forfeiture of retainage as described in Section 40.075.020.040 within this RFP; (2) reduction for consequential and/or liquidated damages as described in Sections 40.075.060 and 40.075.070 within this RFP; and/or (3) credit for retainage not forfeited. The Commonwealth shall pay the invoice minus any reductions including retainage, forfeiture of retainage, and/or damages as set forth in this RFP.

No payment shall be made by the Commonwealth for staff hours expended for modifications up to the amounts specified in Section 30.060.180.030 (Replacement) and Section 30.070.170.060 (Takeover) of this RFP in each State fiscal year under the Operations, Maintenance, and Modifications Phase.

Payment for modification staff hours in excess of those hours allowed in Section 30 of this RFP shall be made as determined by Section 70 within this RFP and Pricing Schedule F.

If, during any operations year, the total number of hours used for modifications is less than the amount specified in Section 30.060.180.030 (25,000 hours) within this RFP, the annual total modification hours minus the actual number of hours used shall be added to the number of hours available for use in the next year. Any unused hours at the completion of the contract will be refunded to the Commonwealth upon the end of the contract period.

Section 40.075.050—Turnover Task

No specific or lump sum payment shall be made by the Commonwealth for Turnover Task services. Payment for such services shall be encompassed in the Operations Task.

Section 40.075.060— Consequential Damages - MEMS System

The Contractor shall, at all times, comply with all system and operational performance standard requirements and expectations specified in this RFP, with Part 11 of the State Medicaid Manual, and with all related Action Transmittals (AT) and Information Memoranda (IM), as well as any modifications or changes thereto and any changes to 42 CFR, 45 CFR, and 95 CFR as they refer to the MMIS and its operations and the use of Contractor services.

The Contractor further understands and agrees that it shall meet all performance standard requirements identified in the RFP during the life of this Contract. The Contractor shall, at all times, operate the KY MEMIS and its activities in conformity with the policies and procedures of the Commonwealth programs.

All requirements described in the RFP shall be subject to monitoring by the Commonwealth or its designee(s). The Commonwealth reserves the right to monitor performance and may exercise such option, at its discretion, without notice. In the event of a failure to meet the Contract or performance standards requirements, the Contractor agrees that the Commonwealth may assess and withhold from payments due its damages for the losses defined in Section 40.075.070 within this RFP, or the consequential damages defined in Section 40.075.060 within this RFP, or retainage as defined in Section 40.075.020.040 within this RFP, at the Commonwealth's discretion.

Section 40.075.060.010—New KY MEMS Operational Start Date—Contract Requirement

The Contractor shall have the New KY MEMS fully operational no later than December 1, 2015.

Section 40.075.060.020—New KY MEMS Operational Start Date—Damages

Compliance with the December 1, 2015 New KY MEMS operational start date is critical to the Commonwealth’s interest. If the Contractor does not fully meet the operational start dates approved in the New KY MEMS DDI Phase Detailed Project Work Plan, then the Contractor shall be liable for all costs incurred by the Commonwealth to continue the Legacy KY MMIS and Contractor operations. The Contractor shall also forfeit all claims for payment of monthly expenses and operational payments for that month and each month thereafter until the Commonwealth approves operational readiness.

Section 40.075.060.030—System Certification—Contract Requirement

The Contractor shall ensure that Federal certification approval for the maximum allowable enhanced Federal Financial Participation (FFP) for the New KY MMIS is achieved within one (1) year of the contractual operational start date and that FFP is retroactively approved to the contractual operational start date. In addition, the Contractor shall ensure that that Federal certification approval for the maximum allowable enhanced FFP for the New KY MEMS is maintained throughout the life of the Contract. Should certification fail to be achieved within one (1) year of the contractual New KY MEMS operations start date, the Contractor shall be liable for any damages resulting from its actions or inactions relating to the lack of certification. Should certification fail to be approved retroactively to the contractual New KY MEMS operational start date, the Contractor shall be liable for any damages resulting from its actions or inactions relating to the loss of maximum allowable enhanced FFP. Should de-certification of the New KY MEMS or any component part of either, occur prior to the end of the Contract period, the Contractor shall be liable for any damages resulting from

its actions or inactions relating to the de-certification and loss of maximum allowable enhanced FFP.

Section 40.075.060.040—System Certification—Damages

For any violation of Section 40.075.060.030 within this RFP, the Contractor shall be liable for the Commonwealth and Federal dollar difference between the maximum allowable enhanced FFP and that actually received by the Commonwealth, including any losses due to lack of or loss of certification. All FFP penalty claims assessed by CMS or other Federal agencies shall be withheld from monies payable to the Contractor until all such penalty claims have been satisfied.

Section 40.075.060.050—United States Department of Health and Human Services (US DHHS) Sanctions—Contract Requirements

The Contractor shall perform all of its Medicaid functions according to the terms and conditions required by the SMM, Part 11.

Section 40.075.060.060—US DHHS Sanctions—Damages

If during the New KY MEMS Operations, Maintenance, and Modifications Phase, CMS imposes fiscal sanctions against the Commonwealth as a result of the Contractor's or any subcontractor's action or inaction, the Contractor shall compensate the Commonwealth the entire amount lost by the Commonwealth by the imposition of CMS sanctions.

Section 40.075.060.070—Correctness of Payments—Contract Requirements

All payments, adjustments, and other financial transactions made through the KY MEMS shall be made on behalf of eligible members to active enrolled providers for approved services and in accordance with the payment rules and other policies of the Commonwealth.

The Contractor shall be liable for the actual amount of all detected erroneous payments identified as a result of Commonwealth or Federal claims reviews or as reported by providers or from other referrals that are a result of incorrect Contractor staff action, inaccurate system data, or inaccurate processing. In addition, the Contractor shall be responsible for all costs associated with correcting the erroneous payments, including costs for re-processing, back-out processing, distribution of corrections, and so forth. Such liabilities shall be withheld from Contractor payments. The Contractor, however, may seek recovery on behalf of the Commonwealth from Providers to whom erroneous payments are made using voluntary refund, offset recovery, or other Commonwealth-approved methods.

In addition, the following requirements are included in correctness of payment:

1. The Contractor shall provide accurate and timely buy-in accretion and deletion based upon the Commonwealth-supplied data and the Commonwealth-approved calculation logic.
2. The Contractor shall provide for processing of managed care capitation payments and management fees in the month-end claims cycle and payment in the first checkwriter of the next month.

The Contractor shall notify the Commonwealth immediately upon discovery of any erroneous payments, irrespective of cause, and prior to initiating appropriate recovery action. The Contractor shall use the change request process to notify the Commonwealth of any system errors that result in a potential Provider erroneous payment.

Section 40.075.060.080—Correctness of Payments—Damages

If an erroneous payment is made to a Provider and that payment is the result of a failure of the Contractor either to use available information or to process correctly, then the Contractor shall be liable for the erroneous payment for which full recovery cannot be made using all reasonable procedures. The Contractor shall notify the Commonwealth immediately upon discovery of any erroneous payments, irrespective of cause. The Contractor shall be responsible for any costs associated with system and operations changes associated with fixing the error(s) that caused the erroneous payment, including costs the Commonwealth or its agents incur associated with re-processing of erroneous data distributed by the Contractor.

The Contractor shall pay to the Commonwealth any portion of an erroneous payment not recouped within one-hundred and eighty (180) calendar days of its receipt of the direction initiating its recoupment. In addition to the amount of the erroneous payment(s), the Contractor shall be liable for interest payments at the prevailing prime beginning from the date of erroneous payment through the date of payment to the Commonwealth. The Contractor shall make such payment to the Commonwealth within seven (7) calendar days of the expiration of the one-hundred and eighty (180) calendar-day timeframe.

The Commonwealth shall not be liable to the Contractor for any erroneous payment due that is not recovered by recoupment from Providers. The Contractor may only initiate independent recovery procedures and actions with the prior written approval of the KY MMIS Contract Administrator once the recoupment process described herein has been completed and a repayment amount remains outstanding. The Commonwealth shall review proposed independent recovery procedures and, if reasonable, shall provide written approval. If the Commonwealth recovers any erroneous payments for which the Contractor has reimbursed the Commonwealth, the KY MMIS Contract Administrator shall notify the Contractor, who shall then submit a standard Commonwealth invoice for the returned amount, less expenses incurred by the Commonwealth during the recovery process.

Section 40.075.060.090—Internal Revenue Service (IRS)—Contract Requirements

The Contractor shall produce and mail out 1099 and/or W9 earnings reports no later than January 31 of each year and report to the IRS no later than March 1, or no later than the extended due date if the Contractor has received approval from the Commonwealth to file for an extension.

Section 40.075.060.100—IRS—Damages

The Contractor shall be responsible for payment of IRS penalties/damages for late distribution of 1099s and/or W9s.

Section 40.075.060.110—Delay or Interruption of Operations—Contract Requirement

The Contractor shall ensure there will be no delays or interruptions in the operation of the KY MMIS and related services caused by any failure, act, or omission of the Contractor.

Section 40.075.060.120—Delay or Interruption of Operations—Damages

Delays or interruptions in the operation of the KY MMIS and related services caused by any failure, act, or omission of the Contractor shall constitute a material breach. Regardless if the Commonwealth elects to terminate this Contract upon such a breach, it is nevertheless entitled to recover:

1. The difference between the cost to the Commonwealth under this Contract and the cost to it under any interim or substitute contract or other method of operation.
2. The liability of the Commonwealth to any third person arising directly or consequentially out of the Contractor's breach and cancellation of this Contract.
3. The cost to the Commonwealth of all actions taken by it to locate and secure a substitute or interim Contractor or method of operation.
4. The loss of FFP.

In addition to the above, the Commonwealth shall reduce the Contractor's compensation by the following amounts:

1. Up to ten thousand dollars ($10,000) per calendar day, or any part thereof, for each of the first ten (10) calendar days of delay or interruption of operation continues.
2. Up to twenty thousand dollars ($20,000) per calendar day, or any part thereof, for each of the next twenty (20) calendar days of delay or interruption of operation continues.

3. Up to thirty thousand dollars ($30,000) per calendar day, or any part thereof, for each additional calendar day of delay or interruption of operation continues after thirty (30) days.

Section 40.075.065— Consequential Damages – Takeover of KYMMIS System

The Contractor shall, at all times, comply with all system and operational performance standard requirements and expectations specified in this RFP, with Part 11 of the State Medicaid Manual, and with all related Action Transmittals (AT) and Information Memoranda (IM), as well as any modifications or changes thereto and any changes to 42 CFR, 45 CFR, and 95 CFR as they refer to the MMIS and its operations and the use of Contractor services.

The Contractor further understands and agrees that it shall meet all performance standard requirements identified in the RFP during the life of this Contract. The Contractor shall, at all times, operate the KYMMIS and its activities in conformity with the policies and procedures of the Commonwealth programs.

All requirements described in the RFP shall be subject to monitoring by the Commonwealth or its designee(s). The Commonwealth reserves the right to monitor performance and may exercise such option, at its discretion, without notice. In the event of a failure to meet the Contract or performance standards requirements, the Contractor agrees that the Commonwealth may assess and withhold from payments due its damages for the losses defined in Section 40.075.065 within this RFP, or the consequential damages defined in Section 40.075.075 within this RFP, or retainage as defined in Section 40.075.020.030 within this RFP, at the Commonwealth's discretion.

Section 40.075.070— Liquidated Damages – Replacement MEMS

The Commonwealth and the Contractor shall agree that the operation of the New KY MEMS in conformity with the Contract provisions is necessary to the proper operation of DMS's programs. These programs are vital to the accurate and expeditious reimbursement of Providers of applicable medical services to eligible members and to assure continued delivery of these services to benefit-eligible members. Timely and accurate performance of this Contract shall be the essence of this Contract.

The Commonwealth and the Contractor shall further agree that while failures to meet certain performance standard requirements under this Contract may or will affect the delivery of medical services either directly or indirectly and may or will result directly or proximately in monetary damages to the Commonwealth, the actual amount of such injury and damage shall be impossible or extremely difficult to calculate.

Therefore, the Commonwealth and the Contractor shall agree that the Commonwealth shall reduce compensation to the Contractor in the instances and amounts hereinafter set forth as determined by the Commonwealth. The Parties also agree that the stated reduction in compensation amounts is reasonable and not punitive.

The KY MMIS Contract Administrator shall issue written notification to the Contractor of each failure to meet a performance standard requirement listed below. The imposition and reduction in compensation shall not affect any other rights of the Commonwealth to enforce or terminate this Contract.

If the Commonwealth elects not to exercise a reduction in compensation clause in a particular instance, this decision shall not be construed as a waiver of the Commonwealth's right to pursue future assessment of that performance standard requirement and associated reduction in compensation.

Section 40.075.070.010—Key KY MEMS DDI Phase Milestone Dates—Performance Standards

The Contractor shall be required to design, develop, test, and implement a New KY MEMS no later than December 1, 2015.

Accomplishment of certain specified New KY MMIS DDI Phase activities by the key milestone dates, as defined in Section 30 within this RFP and established in the approved KY MMIS DDI Phase Detailed Work Plan, shall be necessary to ensure full compliance with the start date.

If, for any reason, the Contractor is delayed in meeting these key milestone dates and a Contract modification to the New KY MMIS DDI Phase Detailed Work Plan is not approved, a reduction in compensation may be assessed. Approval of a Contract or New KY MMIS DDI Phase Detailed Work Plan modification does not waive the Commonwealth's ability to impose damages and/or reductions in compensation if warranted by other terms of the Contract.

The reductions in compensation listed in Section 40.075.070.020 within this RFP shall be in addition to any amounts assessed for delays in meeting the operational start date.

Section 40.075.070.020—Key New KY MEMS DDI Phase Milestone Dates—Reduction in Compensation

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) per calendar day, or any part thereof, for each of the first ten (10) calendar days of delay in meeting a milestone date.

The Commonwealth may reduce compensation up to twenty thousand dollars ($20,000.00) per calendar day, or any part thereof, for each of the next twenty (20) calendar days of delay in meeting a milestone date.

The Commonwealth may reduce compensation up to thirty thousand dollars ($30,000.00) per calendar day, or any part thereof, for each additional calendar day of delay in meeting a milestone after thirty (30) calendar days.

Section 40.075.070.030—New KY MEMS DDI Phase Deliverable Due Dates—Performance Standards

Copies of each deliverable, as defined in the approved New KY MMIS DDI Phase Detailed Work Plan, shall be delivered to DMS, in final form, in the number specified and on the date specified in the approved New KY MMIS DDI Phase Detailed Work Plan. DMS may require up to ten (10) paper copies and one (1) electronic copy of all deliverables. The electronic copy shall be compatible with Microsoft Word or other application software as requested by DMS, and submitted on the Commonwealth-specified media. All deliverables shall be in a format approved by DMS, and meet content and accuracy requirements specified or as subsequently defined by DMS.

Section 40.075.070.040—MEMS DDI Phase Deliverable Due Dates—Reduction in Compensation

The Commonwealth may assess one thousand dollars ($1,000.00) for each calendar day, or any part thereof, that a deliverable is late, which includes providing less than the required copies or delivery on incorrect media.

The Commonwealth may assess an additional one thousand dollars ($1,000.00) for each calendar day, or any part thereof, that a deliverable continues to not meet minimum content requirements or the approved format after its formal rejection by DMS, when appropriate.

Section 40.075.070.050—Key Personnel—Performance Standards

Key personnel commitments contained in the Contractor's proposal for all phases of the contract shall not be changed without prior written approval of the KY MMIS Contract Administrator, unless due to the death, disability, resignation, termination, or military recall or of any key individual. Staffing includes the staff proposed for all key positions required in Section 30.060.260.030 within this RFP at the levels of effort proposed or as specified in the Contract. Contractor must maintain staffing levels throughout the project at ninety percent (90%) or more of the staffing plan agreed to during project planning.

Section 40.075.070.060—Key Personnel—Reduction in Compensation

The Commonwealth may assess up to thirty thousand dollars ($30,000.00) in reduction in compensation for each key personnel proposed in the Contractor’s response to the RFP who is changed for reasons other than death, disability, resignation, termination, or military recall.

The Commonwealth may assess up to an additional one thousand dollars ($1,000.00) in reduction in compensation per Commonwealth business day after the initial twenty-five (25) Commonwealth business days allowed for Contractor to find an acceptable replacement for the key personnel and an acceptable replacement has not provided.

Should the contractor fail to maintain ninety percent (90%) of the mutually agreed to staffing plan for a period exceeding 30 contiguous calendar days, the Commonwealth may assess up to an additional one thousand dollars ($1,000.00) in reduction in compensation per Commonwealth business day after the initial thirty (30) Commonwealth business days allowed for Contractor to find an acceptable replacements to maintain the ninety percent (90%) staffing level.

Section 40.075.070.070—Timeliness of Claims Processing—Performance Standards

The Contractor shall meet the following requirements:

1. Adjudicate ninety-five percent (95%) of all clean claims for payment or denial within thirty (30) calendar days of receipt.
2. Adjudicate ninety-nine percent (99%) of all clean claims for payment or denial within ninety (90) calendar days of receipt.
3. Adjudicate all non-clean claims within thirty (30) calendar days of the date of correction of the condition that caused the claim to be unclean.
4. Adjudicate all claims within twelve (12) months of receipt, except for those exempted from this requirement by Federal timely claims processing regulations.

Section 40.075.070.080—Timeliness of Claims Processing—Reduction in Compensation

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) for each failure to meet any of the requirements set forth in Section 40.075.070.070 during the first month.

The Commonwealth may reduce compensation up to twenty thousand dollars ($20,000.00) assessed for each failure to meet any of the requirements set forth in Section 40.075.070.070 within this RFP in consecutive, subsequent months.

Section 40.075.070.090—Documentation—Performance Standards

The Contractor shall be responsible for providing the Commonwealth with complete, accurate, and timely documentation of all modifications made to the operational KY MEMS. Such documentation shall be in accordance with specifications approved by DMS.

Any changes that occur to the operational system shall be documented according to specifications approved by DMS. Documentation of any such changes shall be provided to DMS.

Section 40.075.070.100—Documentation—Reduction in Compensation

The Commonwealth may reduce compensation up to five hundred dollars ($500.00) for each business day, or any part thereof (beginning the next business day after the documentation due date) that the required documentation has not been provided to the Commonwealth.

The Commonwealth may reduce compensation up to five hundred dollars ($500.00) for each business day, or any part thereof, during which the documentation is unacceptable as to format, accuracy, and completeness based on DMS review. Reduction in compensation may be imposed until the Contractor provides the Commonwealth with acceptable documentation.

Section 40.075.070.110—Online Access to KY MEMS and Response Time—Performance Standards

The Contractor shall provide the Commonwealth staff with online access to all KY MEMS online screens, systems, and data, including all Web-enabled capabilities, between the hours of 7:00 a.m. to 7:00 p.m. Eastern Time (EST or EDT as applicable) on each calendar day for ninety-nine percent (99%) of each month. The Contractor shall maintain the KY MEMS accessibility during other hours, subject to reasonable Commonwealth notification.

Response time shall be less than or equal to three (3) seconds for Commonwealth access to inquiry and update screens.

Section 40.075.070.120—Online Access to KY MEMS and Response Time—Reduction in Compensation

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) for every percentage point below ninety-nine percent (99%) for each month in which Commonwealth does not have online access available as required by Section 40.075.070.110 within this RFP.

The Commonwealth may reduce compensation up to one thousand dollars ($1,000.00) per calendar day for any KY MEMS inquiry or update screen that has a documented response time greater than three (3) seconds.

Section 40.075.070.130—Electronic Claims Submission Availability and Response Time—Performance Standards

The Contractor shall ensure electronic claims submission is available 24x7x365, except for Commonwealth-approved maintenance timeframes. The Contractor shall provide a response for electronic claims submission in three (3) seconds or less, ninety-nine percent (99%) of the time.

Section 40.075.070.0140—Electronic Claims Availability and Response Time—Reduction in Compensation

The Commonwealth shall reduce compensation by up to ten thousand dollars ($10,000.00) per hour when the electronic claims submission or a component of electronic claims submission is not available for provider response for greater than one (1) hour in a calendar day, other than scheduled or Commonwealth-approved down time.

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) for every percentage point below ninety-nine percent (99%) for each month in which the response for electronic claims submission does not meet response time as required by Section 40.075.070.130 within this RFP.

Section 40.075.070.150—Key Turnover Phase Milestone Dates—Performance Standards

The Contractor will be required to provide full support for system turnover activities in accordance with the DMS approved Contractor Turnover Plan as follows:

a. Assistance in turning over the complete and most current KY MEMS to the Commonwealth or its agent.
b. Assistance and support in turnover activities necessary to affect an orderly, structured, smooth turnover to enable DMS and the new vendor achieve successful transition of system operations to a new MEMS system operated by the Commonwealth or its agent.

Accomplishment of certain specified turnover activities by key milestone dates, as established in the Commonwealth-approved KY MEMS Turnover Plan, shall be necessary to ensure full compliance with the start date.

If, for any reason, the Contractor is delayed in meeting these key milestone dates and a Contract Modification to the KY MEMS Turnover Plan is not approved, a reduction in compensation may be assessed. Approval of a Contract or KY MEMS Turnover Plan modification does not waive the Commonwealth's ability to impose damages and/or reductions in compensation if warranted by other terms of the Contract.

The reductions in compensation below shall be in addition to any amounts assessed for delays in meeting the operational start date.

Section 40.075.070.160—Key Turnover Phase Milestone Dates—Reduction in Compensation

The Commonwealth may reduce compensation up to ten thousand dollars ($10,000.00) per calendar day, or any part thereof, for each of the first ten (10) calendar days of delay in meeting a milestone date.

The Commonwealth may reduce compensation up to twenty thousand dollars ($20,000.00) per calendar day, or any part thereof, each of the next twenty (20) calendar days of delay in meeting a milestone date.

The Commonwealth may reduce compensation up to thirty thousand dollars ($30,000.00) per calendar day, or any part thereof, for each additional calendar day of delay in meeting a milestone after thirty (30) days.

Section 40.075.070.170—Turnover Phase Deliverable Due Dates—Performance Standards

Copies of each deliverable, as defined in the Section 30.060.050, shall be delivered to DMS, when appropriate, in final form, in the number specified and on the date specified in the approved KY MEMS Turnover Plan. DMS, when appropriate, may require up to ten (10) paper copies and one (1) electronic copy of all deliverables. The electronic copy shall be compatible with Microsoft Word or other application software as requested by DMS, when appropriate, and submitted on the Commonwealth-specified media. All deliverables shall be in a format approved by DMS, when appropriate, and meet content and accuracy requirements specified or as subsequently defined by DMS, when appropriate.

Section 40.075.070.180—Turnover Phase Deliverable Due Dates—Reduction in Compensation

The Commonwealth may assess up to one thousand dollars ($1,000.00) for each calendar day, or any part thereof, that a deliverable is late which includes providing less than the required copies or delivery on incorrect media.

The Commonwealth may assess up to an additional one thousand dollars ($1,000.00) for each calendar day or any part thereof that a deliverable continues to not meet minimum content requirements or the approved format after its formal rejection by DMS, when appropriate.

Section 40.080—Contractor Cooperation in Related Efforts

The Commonwealth of Kentucky may undertake or award other contracts for additional or related work, services, supplies, or commodities, and the Contractor shall fully cooperate with such other contractors and Commonwealth employees. The Contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Commonwealth employees.

Section 40.085—Subcontractors

The Contractor is permitted to make subcontract(s) with any other party for furnishing any of the work or services herein. The Contractor shall be solely responsible for

performance of the entire Contract whether or not subcontractors are used. The Commonwealth shall not be involved in the relationship between the prime contractor and the subcontractor. Any issues that arise as a result of this relationship shall be resolved by the prime contractor.

All references to the Contractor shall be construed to encompass both the Contractor and any subcontractors of the Contractor.

Section 40.090—Contractor Affiliation

"Affiliate" shall mean a branch, division or subsidiary that is effectively controlled by another party. If any affiliate of the Contractor shall take any action that, if done by the Contractor, would constitute a breach of this agreement, the same shall be deemed a breach by such party with like legal effect.

Section 40.095—Performance Bond

Pursuant to 200 KAR 5:305, the Contractor shall furnish a performance bond satisfactory to the Commonwealth in an amount of ten percent (10%) of the total contract as security for the faithful performance of the Contract. The bond furnished by the Contractor shall incorporate by reference the terms of the Contract as fully as though they were set forth verbatim in such bonds. In the event the Contract is amended, the penal sum of the performance bond shall be deemed increased by like amount.

The initial bond shall be submitted to the Commonwealth Buyer within thirty (30) days of execution of this Contract. Any required amendment to the bond shall be submitted to the Commonwealth Buyer within thirty (30) days of said amendment.

Section 40.100—Commonwealth Property

The Contractor shall be responsible for the proper custody and care of any Commonwealth-owned property furnished for Contractor's use in connections with the performance of this Contract. The Contractor shall reimburse the Commonwealth for its loss or damage, normal wear and tear excepted.

The Contractor will return Commonwealth equipment or facilities, if any.

Section 40.105—Insurance

The Contractor shall provide professional liability insurance for its professional employees, public liability, property damage, and workers' compensation insurance, insuring as they may appear, the interest of all parties of agreement against any and all claims which may arise out of the Contractor's operations under the terms of this Contract. In the event any carrier of such insurance exercises cancellation, notice of such cancellation shall be made immediately to the Commonwealth Buyer.

Section 40.110—Confidentiality of Contract Terms

The Contractor and the Commonwealth agree that all information communicated between them before the effective date of the Contract shall be received in strict confidence and shall not be necessarily disclosed by the receiving party, its agents, or employees without prior written consent of the other party. Such material will be kept confidential subject to Commonwealth and Federal public information disclosure laws.

Upon signing of the Contract by all Parties, terms of the Contract become available to the public, pursuant to the provisions of the Kentucky Revised Statutes.

The Contractor shall have an appropriate agreement with its Subcontractors extending these confidentiality requirements to all Subcontractors' employees.

Section 40.115—Confidential Information

The Contractor shall comply with the provisions of the Privacy Act of 1974 and instruct its employees to use the same degree of care as it uses with its own data to keep confidential information concerning client data, the business of the Commonwealth, its financial affairs, its relations with its citizens and its employees, as well as any other information which may be specifically classified as confidential by the Commonwealth in writing to the Contractor. All Federal and State Regulations and Statutes related to confidentiality shall be applicable to the Contractor. The Contractor shall have an appropriate agreement with its employees to that effect, provided however, that the foregoing will not apply to:

1. Information which the Commonwealth has released in writing from being maintained in confidence;
2. Information which at the time of disclosure is in the public domain by having been printed an published and available to the public in libraries or other public places where such data is usually collected; or
3. Information, which, after disclosure, becomes part of the public domain as defined above, thorough no act of the Contractor.

The Contractor shall have an appropriate agreement with its Subcontractors extending these confidentiality requirements to all Subcontractors' employees.

Section 40.120—Advertising Award

The Contractor shall not refer to the Award of Contract in commercial advertising in such a manner as to state or imply that the firm or its services are endorsed or preferred by the Commonwealth of Kentucky.

Section 40.125— Patent or Copyright Infringement

The Contractor shall report to the Commonwealth promptly and in reasonable written detail, each notice of claim of patent or copyright infringement based on the performance of this Contract of which the Contractor has knowledge.

The Commonwealth agrees to notify the Contractor promptly, in writing, of any such claim, suit or proceeding, and at the Contractor's expense give the Contractor proper and full information needed to settle and/or defend any such claim, suit or proceeding.

If, in the Contractor's opinion, the equipment, materials, or information mentioned in the paragraphs above is likely to or does become the subject of a claim or infringement of a United States patent or copyright, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, with the Commonwealth's written consent, substitute other equally suitable equipment, materials, and information, or at the Contractor's options and expense, obtain the right for the Commonwealth to continue the use of such equipment, materials, and information.

The Commonwealth agrees that the Contractor has the right to defend, or at its option, to settle and the Contractor agrees to defend at its own expense, or at its option to settle, any claim, suit or proceeding brought against the Commonwealth on the issue of infringement of any United States patent or copyright or any product, or any part thereof, supplied by the Contractor to the Commonwealth under this agreement. The Contractor agrees to pay any final judgment entered against the Commonwealth on such issue in any suit or proceeding defended by the Contractor.

If principles of governmental or public law are involved, the Commonwealth may participate in the defense of any such action, but no costs or expenses shall be incurred for the account of the Contractor without the Contractor's written consent.
The Contractor shall have no liability for any infringement based upon:

1. The combination of such product or part with any other product or part not furnished to the Commonwealth by the Contractor.
2. The modification of such product or part unless such modification was made by the Contractor.
3. The use of such product or part in a manner for which it was not designed.

Section 40.130—Permits, Licenses, Taxes and Commonwealth Registration

The Contractor shall procure all necessary permits and licenses and abide by all applicable laws, regulations, and ordinances of all Federal, State, and local governments in which work under this Contract is performed.

The Contractor shall maintain certification of authority to conduct business in the Commonwealth of Kentucky during the term of this Contract. Such registration is obtained from the Secretary of State, who will also provide the certification thereof. However, the Contractor need not be registered as a prerequisite for responding to the RFP. Additional local registration or license may be required.

The Contractor shall pay any sales, use, and personal property taxes arising out of this Contract and the transaction contemplated hereby. Any other taxes levied upon this Contract, the transaction, or the equipment or services delivered pursuant hereto shall be borne by the Contractor.

Section 40.135—Contract Claims

The Parties acknowledge that KRS 45A.225 to 45A.290 governs contract claims.

Section 40.140—Rights and Remedies

The rights and remedies of the Commonwealth provided in Section 40 shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

Section 40.145—EEO Requirements

The Equal Employment Opportunity Act of 1978 applies to All State government projects with an estimated value exceeding $500,000. The Contractor shall comply with all terms and conditions of the Act.

A copy of the EEO forms may be obtained by downloading them from the Finance website at: http://finance.ky.gov/services/eprocurement/Pages/VendorServices.aspx. Select forms under **Attachment #4**. (See Section 50.140 of this RFP for the forms that must be completed and submitted with Technical Proposal). Direct coordination with the EEO Office is approved to discuss EEO requirements and forms. The EEO office's telephone number is (502) 564-2874 and fax (502) 564-1055.

The Commonwealth will review the EEO Forms (or equivalent, if applicable) upon receipt. If a Vendor is under-utilized or in non-compliance, the Vendor shall receive notification from the Commonwealth. The Vendor shall have five (5) days from receipt of such notice to submit an affirmative action plan. Failure to submit an affirmative action plan within the timeframe specified may result in the disqualification of the Vendor's response. In any event, a Vendor shall not be eligible for an award of contract without being in compliance with the EEO requirements.

If the Vendor is exempt from submitting the EEO Forms, the Vendor must state such in its transmittal letter (Section 50.150 of this RFP). Exemption from EEO Form submission, under KRS 45.590, does not obviate any other requirements of KRS 45.570.

Section 40.150—Provisions for Termination of the Contract

Any Contract resulting from this Solicitation shall be subject to the termination provisions set forth in 200 KAR 5:312.

Section 40.160—Bankruptcy

In the event the Contractor becomes the subject debtor in a case pending under the Federal Bankruptcy Code, the Commonwealth's right to terminate this Contract may be subject to the rights of a trustee in bankruptcy to assume or assign this Contract. The trustee shall not have the right to assume or assign this Contract unless the trustee (a) promptly cures all defaults under this Contract; (b) promptly compensates the Commonwealth for the monetary damages incurred as a result of such default, and (c) provides adequate assurance of future performance, as determined by the Commonwealth.

Section 40.170—Conformance with Commonwealth & Federal Laws/Regulations

This Contract is subject to the laws of the Commonwealth of Kentucky and where applicable Federal law. Any litigation with respect to this Contract shall be brought in State or Federal court in **Franklin County, Kentucky.**

Section 40.190—Recycling

The Contractor is required to comply with the recycling requirements of 200 KAR 5:330.

Section 40.200—Funding Limitations

If any or all responses received exceed the amount of funding available, then the Finance and Administration Cabinet, Office of Procurement Services, reserves the right to cancel this RFP.

Section 40.210—Accessibility

Vendor hereby warrants that the products or services to be provided under this Contract comply with the accessibility requirements of section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, part 1194. Vendor further warrants that the products or services to be provided under this Contract comply with existing Federal standards established under Section 255 of the Federal Telecommunications Act of 1996 (47 U.S.C. § 255), and its implementing regulations set forth at Title 36, Code of Federal Regulations, part 1193, to the extent the Vendor's products or services may be covered by that act. Vendor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention.

Section 40.220—State Vendor Eligibility Request Form

Revenue Form 10A100, “State Vendor Eligibility Request Form”, effective July 2008, is a form to be completed by any person or entity wishing to contract with the

Commonwealth to provide goods or services subject to sales and use tax pursuant to KRS 139.200. The form is located at this web-link as Attachment 5:

http://finance.ky.gov/services/eprocurement/Pages/VendorServices.aspx

In accordance with administrative regulation 200 KAR 5:390, this form has to be completed and submitted, before a contract can be awarded. Section 2 of the regulation also notes: "Failure to submit the required documentation or to remain registered and in compliance with the sales and use tax filing and remittance requirements of KRS 139.540 and KRS 139.550 throughout the duration of the contract shall constitute a material breach of the contract and the contract may be terminated."

Section 40.230— Access to Records

The contractor, as defined in KRS 45A.030 (9) agrees that the contracting agency, the Finance and Administration Cabinet, the Auditor of Public Accounts, and the Legislative Research Commission, or their duly authorized representatives, shall have access to any books, documents, papers, records, or other evidence, which are directly pertinent to this contract for the purpose of financial audit or program review. Records and other prequalification information confidentially disclosed as part of the bid process shall not be deemed as directly pertinent to the contract and shall be exempt from disclosure as provided in KRS 61.878(1)(c). The contractor also recognizes that any books, documents, papers, records, or other evidence, received during a financial audit or program review shall be subject to the Kentucky Open Records Act, KRS 61.870 to 61.884.

In the event of a dispute between the contractor and the contracting agency, Attorney General, or the Auditor of Public Accounts over documents that are eligible for production and review, the Finance and Administration Cabinet shall review the dispute and issue a determination, in accordance with Secretary's Order 11-004.

The Vendor shall develop SSAE16 audits once per year, both for the Data Center and for the local facility.

Section 40.240—Funding-Out Provision

The Vendor agrees that if funds are not appropriated to the agency or are not otherwise available for the purpose of making payments, the agency shall be authorized, upon sixty (60) days written notice to the Vendor, to terminate this contract. The termination shall be without any other obligation or liability of any cancellation or termination charges, which may be fixed by the contract.

Section 40.250—Reduction in Contract Worker Hours

The Kentucky General Assembly may allow for a reduction in contract worker hours in conjunction with a budget balancing measure for some professional and non-professional service contracts. If under such authority the agency is required by Executive Order or otherwise to reduce contract hours, the contract will be reduced by the amount specified in that document.

Section 40.255—Registration with the Secretary of State by a Foreign Entity

Pursuant to KRS 45A.480(1)(b), an agency, department, office, or political subdivision of the Commonwealth of Kentucky shall not award a State contract to a person that is a foreign entity required by KRS 14A.9-010 to obtain a certificate of authority to transact business in the Commonwealth ("certificate") from the Secretary of State under KRS 14A.9-030 **unless the person produces the certificate within fourteen (14) days of the bid or proposal opening. Therefore, foreign entities should submit a copy of their certificate with their solicitation response.** If the foreign entity is not required to obtain a certificate as provided in KRS 14A.9-010, the foreign entity should identify the applicable exception in its solicitation response. Foreign entity is defined within KRS 14A.1-070.

For all foreign entities required to obtain a certificate of authority to transact business in the Commonwealth, if a copy of the certificate is not received by the contracting agency within the time frame identified above, the foreign entity's solicitation response shall be deemed non-responsive or the awarded contract shall be cancelled.

Businesses can register with the Secretary of State at:
https://secure.kentucky.gov/sos/ftbr/welcome.aspx.

Section 40.260 – Limitation of Liability

The liability of the Commonwealth related to contractual damages is set forth in KRS 45A.245.

END OF SECTION 40